Int. Journal of Business Science and Applied Management, Volume 2, Issue 2, 2007

SMEs, electronically-mediated working and data security: cause for concern?

Fintan Clear, Brunel University
Brunel Business School
Elliott Jaques Building, Uxbridge, Middlesex, UB8 3PH, UK
Tel: +44(0)1895-672390
Fax: +44(0)1895-269775
Email: Fintan.Clear@brunel.ac.uk

Abstract

Security of data is critical to the operations of firms. Without the ability to store, process and transmit data securely, operations may be compromised, with the potential for serious consequences to trading integrity. Thus the role that electronically-mediated working plays in business today and its dependency on data security is of critical interest, especially in light of the fact that much of this communication is based on the use of open networks (i.e. the Internet). This paper discusses findings from a 'WestFocus' survey on electronically-mediated working and telework amongst a sample of SMEs located in West London and adjacent counties in South-Eastern England in order to highlight the problems that such practice raises in terms of data security. Data collection involved a telephone survey undertaken in early 2006 of 378 firms classified into four industrial sectors ('Media', 'Logistics', 'Internet Services' and 'Food Processing'). After establishing how ICTs and the Internet are being exploited as business applications for small firms, data security practice is explored on the basis of sector and size with a focus on telework. The paper goes on to highlight areas of concern in terms of data security policy and training practice. Findings show some sector and size influences.

Keywords: data security, small firms, ICT adoption behaviour, electronically-mediated working, telework, security policy, security training, sector, firm size

Acknowledgement: The author would like to acknowledge the financial support provided by WestFocus* under the Higher Education Innovation Fund (HEIF 2) and the contributions of the other project team members: David Barnes, Romano Dyerson, G. Harindranath and Wendy Gerrish (all Royal Holloway University of London), Keith Dickson and Lisa Harris (Brunel University), Paul Wallin (Kingston University) and Alan Rae (Ai Consultants). (*WestFocus is a partnership between universities, SMEs and community groups in South and West London and the Thames Valley, UK.)

1 INTRODUCTION

One particular consideration that firms must account for whilst engaged in electronically-mediated working is the security of data. Any standard text will argue that a security system can only be as strong as its weakest link. In a field that is notoriously difficult to obtain authoritative data, the WestFocus research project 'ICT adoption and use by SMEs' reported on in this paper attempted to gain empirical evidence *inter alia* on the manner in which SMEs balance security considerations with networked working and trading.

Data security was defined in 1992 by NISS as the "protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure". McLeod and Schell (1997) maintain that data security requires three aspects to be maintained: integrity (i.e. providing an accurate representation of the physical reality that data represents); availability (i.e. allowing those authorised to have access to data); and confidentiality (i.e the protection of data and information from disclosure to unauthorised persons). Without the ability to store, process and transmit data securely, operations may be compromised for which there can be very detrimental consequences for trading. Thus the role that electronic communications play in business today and its dependency on data security is of critical interest. Much of this communication uses open network protocols on an Internet whose underpinning technology was originally designed for sharing data in research projects rather than for the purposes of e-commerce (Ratnasingham, 1998). Given typical assertions that to retain competitive edge firms must develop e-business processes that span more than one organisation (Nah *et al*., 2004), then firms so minded are obliged to exercise some level of oversight for data handling across electronically-enabled communications domains that extend beyond the internal. However apart from purely working with primary suppliers and customers in electronic alliance, firms are increasingly outsourcing tasks such as network support to 'third parties' (Gupta and Hammond, 2005) in electronic networks that may demand 'flexible workers' to have ubiquitous access (i.e. at any place and at any time using fixed and/or mobile modes) to both their own information systems and those of trading partners. With Spinellis *et al.* (1999) arguing that advanced technology has in many cases outpaced the development of 'control practice and employee knowledge', it is clear that the greater use of electronically-enabled communications may pose complex challenges for data security.

While much of the academic literature focuses on large firms, much less is evident on the experiences of SMEs in terms of ICT usage (Martin and Matlay, 2001; Dixon *et al.*, 2002) or on the emergence of networked trading which proponents such as Straub (2002) argue is becoming the dominant commercial paradigm. Clear and objective evidence on how small and medium-sized enterprises (SMEs) exploit ICTs and the Internet and the concommitant threats to data security need to be continually updated if policy makers, small firms and the technology providers that supply them are to work with the world as it really is, rather than as it may be portrayed on occasion by some technology providers. According to Simpson and Docherty (2004), distrust felt by owner/managers in the effectiveness of government-sponsored business support mechanisms conspires to add to a problem whereby small firms' ignorance of new technologies and systems makes them capable of their being exploited by technology providers. So in the absence of authoratative and objective voices informing small firms of market realities, unchecked commercial imperatives felt by organisations supplying the market with ICT-related tools may lead them to overstate threats in order to sell their wares, perhaps causing "firms (to) continue to choose technologies which may not be very effective for their environment" (Gupta and Hammond, 2005, p. 307). In findings from case studies of eight firms (of various sizes), Nathan *et al.* (2003) note poor ICT procurement practice whereby senior management purchase information systems that they do not fully comprehend, to then foist on an untrained staff which results in the sub-optimal use of those systems and what they call 'low-tech equilibrium'. Such a backdrop may do little to establish clarity for firms trying to work in a digital realm, and in all likelihood may conspire to confuse and hence to compromise data security policy and practice. Arguably, this constitutes a market failure.

There are over 4 million enterprises in the UK (DTI, 2003). The majority of these - nearly 3 million – are 'one-man-bands' (i.e they have no employees) leaving around 1.1 million which have employees. Further breakdown shows that 960,000 have between one and nine employees (constituting 'micro firms'), 160,600 have between 10 and 49 employees ('small firms'), 26,000 have between 50 and 249 employees ('medium-sized firms') and just over 6,000 have 250 employees and above ('large firms'). Thus SMEs – firms with between 0 and 249 employees - account for over 99 percent of all businesses in the UK, and thus have a significant role to play in the UK economy (Beaver, 2002). For the purposes of this study however, firms with no employees (i.e. single operators or 'one-man-bands') have been excluded. Exploration of sector and size differences will be undertaken therefore on the basis of firms with employees only.

The paper begins with a review of the literature, followed by an introduction of the WestFocus research project and methodology. Next research findings are set out, beginning with data on how ICTs and the Internet are being exploited by the SME sample in inter-firm trading. After setting out the general e-trading background for the sample as a whole, the discussion moves on to consider 'offsite working' or 'telework' with sector and firm size comparisons, followed by consideration of security policy and practice, again based on sector and size data. Then come concluding remarks.

2 LITERATURE REVIEW

There is a small but growing literature on e-business adoption taking a small firm perspective, some of which contains discussion on security risks. One focus whilst looking at adoption is on drivers, promoters or advantages of e-business (Poon and Swatman, 1999; Riemenscheider and McKinney, 2001; Shiels *et al*., 2003; Simpson and Docherty, 2004; Fillis *et al*., 2004; Stockdale and Standing, 2004 & 2006; MacGregor and Vrazalic, 2005) and barriers, hurdles or inhibitors (Riemenscheider and McKinney, 2001; Levy and Powell, 2003; Simpson and Docherty, 2004; Fillis *et al*., 2004; Stockdale and Standing, 2004 & 2006; Taylor and Murphy, 2004; MacGregor and Vrazalic, 2005). In a 2002 literature review of the area Dixon *et al*. (2002) identify common aspects found in relation to e-business adoption barriers for SMEs. Concerns for security and privacy is one such in a list that also contains a generalised lack of awareness of the potential of ICT, a lack of an IT skills base, concerns for high initial set-up costs, and a lack of staff to implement ICT. The general depth of discussion on security issues however in this literature is limited as noted in Appendix 1. Thus some authors spend a paragraph discussing the subject while others do little more than mention it. So while the subject of security is often raised in this literature, it lacks in-depth examination.

Researchers note the heterogeneity of SMEs (Martin and Matlay, 2001; Dixon et al., 2002; Taylor and Murphy, 2004), and sector and size examinations have been made of SME ICT and e-business adoption. Results are conflicting in places. Simpson and Docherty (2004) find sector to be a significant factor in e-business adoption and Martin and Matlay (2001) add that a micro-business focusing on business services is more likely to adopt ICT than a similar-sized manufacturing firm. Levy and Powell (2003) on the other hand find little evidence on the basis of sector for differential patterns in ICT adoption. Similarly, Van Beveren and Thompson (2002), MacGregor and Vrazalic (2005) and Levenburg (2005), argue that firm size is a significant factor in e-business adoption while Levy and Powell (2003) argue, in relation to ICT adoption, that size is not significant.

Another focus in this literature is on adoption models with a number being critical of stage models (which include the 'DTI Adoption Model') (Martin and Matlay, 2001; Levy and Powell, 2003; Fillis *et al*., 2004; Taylor and Murphy, 2004) on which UK business support has been based. These authors see stage models as prescriptive and ill-fitting of actual small firm adoption behavior. Simpson and Docherty (2004) are particularly critical of some business support mechanisms as delivered on the ground and based on the stage model paradigm; Levy and Powell (2003) argue for a 'contingent' approach in which adoption behavior is seen to be based more on apparent business need than on a linear and apparently seamless progression towards some vaguely-defined 'digital nirvana' where pervasive and integrated operations are transacted between and amongst firms. Ill-fitting policy can help contribute to distrust of government support agencies by small firms as Simpson and Docherty (2004) note with the potential effect of inhibiting small firms from seeking what should be 'disinterested' advice on critical issues such as data security. However MacGregor and Vrazalic (2005) find some taxonomies 'manufactured' (p. 511) and reflections of research design rather than reality on the ground. Citing Watson *et al*. (2000), Fillis *et al*. (2004) appear highly critical of the academic literature by warning of "the continued belief by many researchers in the sole value of formalised, structured, prescriptive ways of conceptualising business behavior despite the realities of non-linear, sometimes chaotic behavior" (p.350).

From an intra-firm 'distributed working' or 'telework' perspective, there is still however a paucity of in-depth academic research that looks into data security *per se* let alone one taking a small firm perspective. Aside from arguments on its efficacy, much writing on telework examines management issues raised by telework or, as for e-business, examines barriers inhibiting its adoption. So Lim and Teo (2000) in a commentary on ICT use in teleworking spend one paragraph discussing the risk of confidential data loss. Authors who take a more distinct focus on data security include Gupta and Hammond (2005) who examine IS security issues in small businesses. Echoing Spinellis *et al*. (1999) they go on to highlight resources as an issue for small firms where data security is concerned, and observe that 49% of organisations in the U.K see budget constraints as having some prime influence on 'computer security implementations'. They detail constraints felt by small firms in relation to security as: lack of staff with security expertise; lack of financial resources to hire expert help or to provide

training; lack of understanding of risks or being dismissive of them; inability to focus upon security due to other business priorities (Gupta and Hammond, 2005).

Authors directly examining telework and data security issues however are Sturgeon (1996) and Spinellis *et al*. (1999). Sturgeon identifies risks such as individual teleworkers handling sensitive data from home; Spinellis *et al.* who compare home office security threats with those of small firms examine the use of networked information systems (IS) within small businesses and home offices. They go on to argue that each shares a similar lack of technical expertise and resources by which to create and maintain a security posture adequate to apparent threat. Both studies argue for use of risk assessment procedures to minimise such threats. Amongst sometimes dated recommendations, Nilles (1998) argues for strong methods of user authentication and for network design principles that reflect a heterogeneity of access modes. Rikitake *et al.* (2001, 2002a, 2002b) examine data security issues raised by technologies such as WLANs, teleconferencing, P2P and VoIP in telework. They point, for example, to the risk of other family members using the same home PC and accessing, perhaps, Peer-to-Peer (P2P) networks which are known to be risky due to the possibility, they imply, of picking up computer viruses and other malware (2001). A US government-sponsored study (Kuhn *et al*., 2002) on telecommuting points to vulnerabilities in, amongst others, wireless networking, web browsers and printing software.

More typical of the literature are telework studies which have distinct foci other than security, but which note data security vulnerabilities as part of their examinations. Thus Clear and Dickson (2005) in a study on how management attitudes and levels of worker autonomy shape telework adoption in small firms discuss risks to data security in terms of its being a major disadvantage to the adoption of telework. Fulton *et al.* (2001) in a study on 'home-based e-work' that examines the blurring of home and work boundaries identify the shared use of home PCs as being a source of risk for data security. Tremblay (2002) explores work-life balance issues, but points to the dissatisfaction expressed by teleworkers of cumbersome security procedures. An Australian study (Standen and Sinclair-Jones, 2003) notes security issues raised by outsourcing and the development of a globalised service sector workforce. They go on to promote the use of 'ethical hackers' who can be employed to test network defences. Illegems and Verbeke (2003) argue that one of the factors militating against telework adoption is that it 'hinders the security of internal data' (p. 79) with two possible forms of unauthorised access defined: industrial espionage and intrusion by employees. They also argue that any form of telework implementation that leads to employees becoming self-employed freelancers will raise the level of risk to internal data as loyalty to their firm will diminish. Tran and Atkinson (2002) argue that privacy and security processes are required for multinational firms transferring data across international borders. Given the complexities of the issues inherent in the protection of data security, Lohmeyer *et al*. (2002) argue that IT departments should employ managed security providers (MSPs) to help them face security challenges online.

There are a number of guides offering advice on 'good practice' in relation to data security when working in a distributed and electronically-mediated manner and three are noted here. Huws and Podro (1995) argue that teleworkers should be trained to protect data security through anti-virus software, password use and taking back-ups of work-in-progress; if such training were not forthcoming, then teleworkers should not be held responsible for losses of data. The 'UK Online for Business' publication 'Working Anywhere' (2000) points out that safe data handling is dependant not just on technical measures and procedures but also on having reliable and vetted staff. Kuhn *et al.* (2002) argue that telecommuting staff working for US federal bodies should be given guidance on selecting appropriate technology, software packages and tools in order for best practice in data security to be followed.

However most of these authors are not reporting on small firms *per se*, and thus there is a hole in the literature given small businesses are not simply 'scaled-down versions' of large businesses (Quayle, 2004; MacGregor and Vrazalic, 2005). Numerous writers note that small firms face resource constraints not necessarily faced by large firms (Poon and Swatman, 1999; Levy and Powell, 2003; Simpson and Docherty, 2004; Fillis *et al*., 2004; Gupta and Hammond, 2005. Smith and Rupp (2002) (cited in Gupta and Hammond, 2005) note that that smaller organisations may place a more limited value on information and its security than larger ones. So though Walden (2005) echoes assertions by Schneier (2000, 2003) that data security issues are not properly understood or given adequate attention in many organisations – i.e. irrespective of size - for theory on SMEs to be relevant, consideration of their "motivations, constraints and uncertainties" (p. 18) must be made which are different in comparison to their larger cousins (Westhead aand Storey, 1996).

Questions of data security are raised amongst other aspects by differing modes of access (fixed versus wireless) and in terms of the variegation of devices (including PCs, personal digital assistants (PDAs) and mobile phones/cell phones) with writers such as Ghosh and Swaminatha (2001) arguing

that mobile commerce raises new security and privacy risks. Nevertheless, whatever the technologies and use of protocols that may protect data security whilst in transit across electronic networks, Gordon (2004) tempers any technology obsession by arguing that "If employees can walk out of the door of those organizations with reports, drawings, diskettes, files, and anything else in their pockets or briefcases (as they almost always can), then it's incorrect to say that telecommuting presents a new and different risk". Apart from deliberate intent by individuals to compromise the security of data, Lundegaard argues that "Disruptions of information systems are mostly a result of human error, ranging from system integration mistakes to accidental cutting of fibre optic cables, and natural disasters..." (Lundegaard, 1997). Whatever the source of risk, Reuvid (2004) argues that management controls and processes overseeing security are critical factors for firm survival. Thus Higgins (1999) observes, "a policy is the start of security management" (p. 217) and that "Effective security management … is based on the systematic concept, dissemination and operation of an information security policy". In the absence of such a policy, businesses may be seen as vulnerable, whether as the result of accident or malevolence. So a firm having a policy suggests that at least some appraisal has been made of potential security threats, however imperfect.

In sum, there are a limited number of studies taking a small firm perspective that focus on security issues raised by electronically-mediated working. As a whole the SME literature offers a sketchy view of security risks faced by small firms in a virtual domain. Amongst a growing volume of studies looking at ICT and e-Business adoption that account for SME experience, a number focus on the 'drivers' and 'barriers' to adoption and/or adoption models, sometimes with sector and firm size consideration. Often security is noted in taxonomies of barriers, but the depth of analysis is such that in many parts the subject appears more mentioned than discussed. A strong critique is made of stage models and in particular the ICT adoption model used by the DTI to underpin UK business support policy. Discussion on the impact of such policy on data security issues however is not very apparent in this literature. A number of writers argue for small firms to start to use risk management methods by which to face up to e-Business security challenges. Nevertheless a persistent reminder in this literature is that a small firm perspective requires consideration of resource constraints. So the literature individuating telework that examines data security is limited Thus other studies, some taking a small firm perspective and some not, need to be sought out for relevant analysis on data security issues within virtual domains.

3 METHODOLOGY

The research findings discussed in this paper are derived from a telephone survey of 378 firms located in a region bounded by West London boroughs and adjacent counties. This involved use of a structured questionnaire of 51 questions which collected data on a broad range of company activities related to ICT adoption and use, including ICT strategy, implementation, investment, training and security policy. As part of a collaborative effort by researchers from Royal Holloway, Kingston and Brunel universities, the target for this phase of a WestFocus project examining 'ICT adoption and use by SMEs' was for 400 completed interviews on the basis of 100 firms each from four industry sectors. These sectors are 'Media', 'Logistics', 'Internet Services', and 'Food Processing', all seen as making significant economic contributions to the study region. Listings of firms for the sectors were obtained from a commercial database provider, and these were sampled until the survey team obtained 100 interviews per sector. The telephone survey took between 20 to 30 minutes to complete, and was undertaken between January and March 2006. Upon completion of the survey, detailed examination of the data by the analysis team led to a certain number of interviews being removed to create a final sample of 378 interviews.

Univariate analysis using SPSS was undertaken of the WestFocus dataset by use of frequency distributions for the whole dataset and by use of cross-tabulations of data by sector and size and other variables. The Chi-square test is applied to these cross-tabulations, and the significance measure is displayed in footnotes. If the Chi-square test shows a lack of significance, then such data is ignored.

According to an European Commission (2002) definition, a Small and Medium-sized Enterprise (SME) has between zero and 249 employees, has a turnover of less than 50 million Euros, and is no more than 25% owned by a non-SME (not including banks or venture capitalists). Due to difficulties in establishing ownership patterns, and getting accurate turnover data, one limitation of the empirical work in this paper is that data has been gathered on firms on the basis of employee numbers only.

As can be seen in Table 1 which shows breakdown of the survey sample by size and sector, the sample is composed of 100 firms from the 'Logistics' and 'Food Processing' sectors, 90 firms from the 'Media' sector, and 88 firms from the 'Internet Services' sector, making 378 firms in the dataset as a whole. By size the sample is composed of 205 'micro firms' (1-9 employees), 140 'small firms' (10-49

employees) and 33 'medium-sized firms' (50-249 employees). The comparatively low number of medium-sized firms in the WestFocus sample overall and the relatively low number of 'Media' (3) and 'Internet Services' (5) firms in this size category act as research limitations. Apart from other considerations, any cell with frequency data lower than five invalidates the Chi-square significance test. Any data in cross-tabular analysis that fails this test is ignored. Thus findings shown in this paper are sometimes constrained to present only partial representations of size and sector data.

Table 1: Survey Sample Breakdown by Size and Sector

		Firm Size			
		Micro	**Small**	**Medium**	**Total**
Sector	**Media**	60	27	3	90
	Logistics	49	38	13	100
	Internet Services	49	34	5	88
	Food Processing	47	41	12	100
	Total	205	140	33	378

4 FINDINGS

The data examined in this section show various findings from the survey. Some of the data is shown on the basis of the whole sample, while other data is shown with breakdown by sector and size. The first findings examined are related to technology use, and this is followed by an examination of 'offsite working' and security policy and practice.

Table 2: Technology Use for Whole Sample

Technology	*%*
Email	99%
Internet	99%
Anti-virus software	96%
Firewall	93%
Own computer network (LAN/WAN)	86%
Broadband	84%
Company Website	84%
Wireless access	53%
Intranet	40%
Extranet/EDI	31%
Video/audio-conferencing	27%
Groupware	23%

Table 2 shows frequency data for a series of technologies and their use by the whole sample. Email (99%) and Internet (99%) use are practically ubiquitous, followed closely by anti-virus software (96%) and firewalls (93%). Own computer network (86%), use of broadband (84%) and company websites (also 84%) also have relatively high levels of adoption. Wireless access is used by 53% of firms, a notable level of adoption given the amount of time that such access has become available. 40% of the sample use intranets and 31% use extranet/EDI technology. Video/audio-conferencing (27%) and Groupware (23%) are the least pervasive technologies in the list.

Levels of use of anti-virus software and firewalls almost mirror email and Internet ubiquity, and taken together suggest that firms are aware of Internet-borne threats and thus take measures to protect themselves. While each of these firms can demonstrate apparent intention, whether their infrastructures are actually secure (to some nominal 99.9% level) is not clear. So a limitation of the data is that evidence that might contradict this picture such as whether firewalls are mis-configured and the level of currency of anti-virus software (i.e. how up-to-date it is) was not obtained as part of the survey. Additionally this data is obviously based at the level of the firm and does not account for practice by individual employees. That said, other technologies of note in terms of distributed working are video/audioconferencing – used by 27% of the sample – and groupware – used by 23%.

Table 3 shows frequency of response to the question, "Do you use the Internet to…?" (and individual options shown in the table) for the sample as a whole. According to these figures it is arguable that 'networked trading' is an established phenomenon in supply chains with customer-facing (downstream) use being more prevalent than supplier-facing (upstream) use. Figures for trading are 58% and 50% respectively in terms of customers and suppliers. A surprising finding is the relatively high level of the use of the Internet to make payments, with 61% of firms receiving payment from customers and 56% of firms making payment to suppliers. Notably 44% of firms use the Internet to work with other firms on collaborative ventures.

Table 3: Use of Internet for Trading Purposes

Trading Purpose	%
Receive payments from customers	61%
Trade with customers	58%
Make payments to suppliers	56%
Trade with suppliers	50%
Work with other firms on collaborative ventures	44%

As numerous commentators including Ratnasingham (1998) argue, trust is a vital element in the take-up of electronically-mediated trading. Allowing access by trading partners to a firm's systems requires, arguably, a high level of trust on the part of the 'provider' to the 'user' (Straub, 2002). Table 4 shows frequency of response to the question "Do you allow remote access to your systems / databases by customers / suppliers / joint venture partners?". Only 11% of the sample allow customers remote access with 6% allowing such access by suppliers and 5% doing so by joint venture partners. The figures are too low for meaningful statistical examination by size or sector. Thus the overwhelming majority of firms in the survey sample do not allow trading partners, whether customers, suppliers or joint venture partners, to have remote access to their systems. While these findings do not in themselves shed light on the issue of trust and any inherent data security risks whilst working in an electronic realm, or, for that matter, on the availability or otherwise of appropriate and cost-effective technology, this data does suggest that close electronic working across supply chains is still rare amongst SMEs.

Table 4: Remote Access to a firm's systems / databases by trading partner

Trading partner	%
Customers	11%
Suppliers	6%
Joint venture partners	5%

Attention now shifts to challenges faced by firms undertaking electronically-mediated trading. Table 5 shows frequency of response for the whole sample to the question "Have you experienced any of the following challenges in developing e-commerce for your business?" As surveyed firms could respond to more than one of the options offered, the data is not mutually exclusive. Of greatest relevance to the concept of 'distributed trading/working' are the responses 'Customers do not want to change' (19%), 'Suppliers are not ready for electronic business' (10%) and 'Difficulties with information sharing in collaborative ventures' (8%). For those promoting the greater use of electronically-mediated trading, such data must offer succour given the relatively low response rate for these challenges as a whole. From the data security perspective, the responses 'Security failures / problems' (6%) and 'Internet fraud' (8%) are most relevant. Though not identical in description, this latter finding chimes with the "Theft or fraud involving computers" finding from the DTI security breaches survey of 8% (DTI, 2006). Again such findings will offer succour to promoters of electronically-mediated trading. However, getting reliable statistics on security issues is difficult (Smith *et al*. 2002 cited in Walden, 2005), therefore figures on the subject should always be approached with caution.

Table 5: E-commerce challenges

E-commerce challenge	%
Customers do not want to change	19%
Difficulty in getting good technical advice from outside	15%
High costs to develop / maintain the web site	14%
Difficulty in hiring staff with appropriate IT skills	13%
Suppliers are not ready for electronic business	10%
High connection costs	8%
Difficulties with information sharing in collaborative ventures	8%
Internet fraud	8%
Security failures / problems	6%

Moving on to a sectoral examination of technology use, data failing the Chi-square 0.05% significance test was removed from consideration. Thus Internet, email, firewall and anti-virus software – all of near-ubiquitous use – are ignored for further analysis. Technologies explored in Table 6 therefore are 'Broadband' (84% adoption rate for the whole sample), 'Wireless Access' (53%) 'Intranet' (40%), 'Extranet/EDI' (31%) and 'Video/Audio-conferencing' (27%). Within the 84% overall adoption rate for Broadband, there is a high of 94% for 'Media' and a low of 81% for 'Food Processing'. This is the only case in which 'Internet Services' (84%) is not the lead adopting sector. So while 81% of the 'Internet Services' sample has wireless access, a notably high figure, the other three sectors show rates of 50% and less. This pattern of adoption is repeated for the three remaining technologies with 'Internet Services' firms running ahead of 'Media', 'Logistics' and 'Food Processing' at adoption rates that are significantly greater. So while 68% of the 'Internet Services' sample uses an intranet, the other three sectors' figures are 38% and less; while 50% of 'Internet Services' uses 'Extranet/EDI', the other three sectors' figures are 34% and less; and while 56% of 'Internet Services' uses 'Video/Audio-conferencing', the other three sectors' figures are 32% and less. Though the figures for the other three sectors are much more bunched, 'Logistics' is shown to be the least-adopting sector for four out of the five technologies. 'Media' appears to slightly lead 'Food Processing' in overall adoption rates for the five technologies which are not much greater than 'Logistics'.

While the data shown here does not show relative use of the technologies by firms in the sample, nevertheless they suggest that electronically-mediated working is practised to relatively high levels by the sample as a whole, and particularly by 'Internet Services'. Even if it may come as no surprise that this sector leads the pack given the nature of their business, it is still sobering to recall that the Internet as a business tool emerged little over 10 years ago.

Table 6: Technology Subset Use by Sector

Technology	**Media**	**Logistics**	**Internet Services**	**Food Processing**
Broadband	94%[1]	78%	84%	81%
Wireless access	48%	35%	81%	50%
Intranet	38%	36%	68%	28%
Extranet/EDI	21%	20%	50%	34%
Video/Audio conferencing	32%	14%	56%	16%

Having established some ICT adoption and use patterns for the sample as a whole and by sector, attention is now drawn to the firms' use of 'offsite working' and security policy and practice. While there are other measures that can be used to evaluate apparent preparedness in data security terms (e.g. policy noted in a staff handbook or employee contract or as part of an induction process), due to the necessity for economy in the survey, two questions were put that were adjudged to be more revealing in these terms. These are "Does your company have a written security policy for employee use of IT?" (referred to in Table 7 as 'Written security policy') and "Do your employees get training to make them aware of IT security issues?" (referred to in Table 7 as 'Security Training'). The other question "Do any of your company's personnel work offsite with access to your information systems (or

[1] Missing data for 1 firm

'telework')?" is referred to in Table 7 as 'Offsite working'. This latter question was so framed in order to avoid possible confusion over sole use of the term 'telework' which the author had experienced in previous research on the subject (Dickson and Clear, 2003). Arguably working offsite '….with access to your information systems' is a reasonable synonym for 'telework' in any event. For the sample as a whole, 51% responded in the affirmative to the question on 'Offsite working'. However when cross-tabulating with 'sector', for three of the four ('Media', 'Logistics' and 'Food Processing') the proportion of firms denying having 'offsite working' in these terms was greater than those having it, with responses of 45%, 37% and 43% respectively. Only 'Internet Services' had a greater proportion of 'offsite working' (82%) than not.

Table 7: 'Offsite working', 'Written security policy' and 'Security training' by Sector

	Sector			
	Media	**Logistics**	**Internet Services**	**Food Processing**
'Offsite working'[2]	45%	37%	82%	43%
Written security policy[3]	30%	32%	53%	45%
Security training[4]	46%	40%	79%	51%

In terms of security policy, as noted above, if management controls and processes are important for a firm's survival (Reuvid, 2004), then to manage data security some form of policy will be required (Higgins, 1999). Policies can be formal or informal, but in order to gather definitive data on the issue, a focus was placed on whether firms had a written and therefore formal security policy or not. With 40% of the whole sample answering 'yes' to this question, breakdown by sector shows that only 'Internet Services' (53%) had a greater proportion of those with a written security policy than not. This suggests that 'Internet Services' firms are generally more aware of the need for data security than the other sectors though 'Food Processing' (45%) is not far behind. However, that said, it may be surprising given the nature of their business that the proportion of 'Internet Services' firms having a formal policy is not even higher.

If having a written security policy demonstrates management commitment to data security in theoretical terms, then devoting time and effort to awareness training of staff on IT security issues may be seen as putting theory into practice to some extent. Across the whole sample, 53% answered 'yes' to the question on security training. 'Internet Services' and 'Food Processing' have a greater proportion providing such training than not, with the converse true for 'Media' and 'Logistics'. 'Internet Services' (79%) firms provide much more training than 'Food Processing' (51%), 'Media' (46%) and 'Logistics' (40%). All sectors show greater levels of 'security training' than 'Written security policy' use. However sector heterogeneity is shown elsewhere: figures for 'offsite working' are greater than 'written security policy' for 'Internet Services', 'Media' and 'Logistics' while for 'Food Processing' the opposite is true; figures for 'offsite working' and 'security training' are similar (+/- 1% and 3%) for the same three sectors with the least similar being for 'Food Processing' (where 'security training' exceeds 'offsite working' by 8%). So arguably the 'Food Processing' sector shows some different adoption behavior here from the other three.

Table 8: 'Offsite Working', 'Written security policy' and 'Security training' by Firm Size

	Size		
	Micro	**Small**	**Medium**
'Offsite working'[5]	42%	57%	84%
Written security policy[6]	26%	53%	74%
Security training[7]	46%	60%	64%

Table 8 shows cross-tabulations between frequency of response to the same three questions as noted above for Table 7 but on the basis of firm size. As noted, the overall number of 'medium-sized

[2] Missing: 11 ('Media': 2; 'Logistics': 1; 'Internet Services': 4; 'Food Processing': 4); Chi-square significance: .000
[3] Missing: 6 ('Media': 1; 'Logistics': 1; 'Internet Services': 2; 'Food Processing': 2); Chi-square significance: .004
[4] Missing: 7 ('Media': 1; 'Internet Services': 4; 'Food Processing': 2); Chi-square significance: .000
[5] Missing: 11 (Micro: 5; Small: 4; Medium: 2); Chi-square significance: .000
[6] Missing: 6 (Micro: 5; Small: 1); Chi-square significance: .000
[7] Missing: 7 (Micro: 5; Small: 2); Chi-square significance: .016

firms' in the whole sample (33) is much smaller than 'small firms' (140) and 'micro firms' (205). If we can accept this as a limitation, then there is an evident size effect in the data for the three questions. Responses to the question on 'offsite working' show affirmative figures of 42% for 'micro firms', 57% for 'small firms' and 84% for 'medium-sized firms'. Responses to the question on 'written security policy' show that 26% of 'micro firms', 53% of 'small firms' and 74% of 'medium firms' have written security policies. This finding chimes with DTI (2006) findings (commented on below) which found that "larger companies remain more likely to have a security policy" (p. 7) with 60% of UK businesses having no formal security policy (Walden, 2005). The final question on 'security training' shows that more 'small firms' and 'medium-sized firms' offer such training than not, with 'micro firms' showing the converse: 64% of 'medium-sized firms' and 60% of 'small firms' offer this training while only 46% of 'micro firms' do so. A 'switchover' is evident in this size data: higher rates of training is recorded than use of a formal security policy for 'micro' and 'small' firms but this is in the reverse for 'medium' firms.

Table 9: Training for Awareness of IT Security Issues v 'Offsite Working'

		'Offsite Working'?		
		Yes	**No**	**Total**
Training for awareness of IT security issues?[8]	**Yes**	32%	21%	53%
	No	19%	28%	47%
	Total	51%	49%	100%

At this point, consideration is turned to direct comparison between levels of training on IT security awareness and 'offsite working' (or 'telework') on the basis of the whole sample. Table 9 shows a cross-tabulation of frequency of response to the questions "Do any of your company's personnel work offsite with access to your information systems (or 'telework')?" and "Do your employees get training to make them aware of IT security issues?". Proportions shown are noted for a total sample of 364 responses[9]. The table shows that 51% of the total sample have 'offsite working' and 49% not with 53% of the total sample having training on IT security awareness and 47% not. Cross-tabulating these two variables shows that 32% of the sample have both 'offsite working' *and* training on IT security awareness while 19% have 'offsite working' *and no* security training. Put another way, 37% of the firms with 'offsite working' do not have security training.

Table 10: Written Security Policy v 'Offsite Working'

		'Offsite Working'?		
		Yes	**No**	**Total**
Written Security Policy?[10]	**Yes**	28%	12%	40%
	No	23%	36%	60%
	Total	51%	49%	100%

Table 10 shows a cross-tabulation of frequency of response to the questions "Do any of your company's personnel work offsite with access to your information systems (or 'telework')?" and "Does your firm have a written security policy for employee IT use?" 28% of the responses show firms with both 'offsite working' and a written security policy, but 23% of those firms having 'offsite working' do not have a written security policy. Put another way, 45% of the firms that have 'offsite working' have no formal security policy.

[8] Missing: 12; Chi-square significance: .000

[9] On a methodological note, from this point findings for total numbers of responses may differ with those cited in sections above. So whereas the number of those having 'offsite working' noted above is 367 (with missing data for 11 firms), and the equivalent number for 'training for awareness of IT security issues' is 371 (with missing data for 7 firms), the confluence of data for these two responses produces a total of 364. If data is missing for either question, then that case will be ignored for analysis purposes. Variability of totals for the same question between different cross-tabulations is explained by the fact that missing data can be mutually exclusive (i.e. where data is missing for one question only) or mutually inclusive (i.e. where data is missing for both questions).

[10] Missing: 13; Chi-square significance: .000

Now cross-tabulation of the data is attempted using three variables. However a lack of statistical significance reported by SPSS for the Chi-square test renders some cross-tabulations invalid. Cross-tabulating the training variable with formal policy and 'offsite working' variables is one such enquiry, so is ignored from further consideration. Therefore attention is drawn to use of a formal security policy and 'offsite working' by size and sector, though here too there are limitations. Failure of the Chi-square significance test is also the case for 'medium' firms so cross-tabulation of 'written security policy' and 'offsite working' data (as shown in Table 10) by firm is restricted to 'micro' (Table 11) and 'small' (Table 12) views. Table 11 shows that 42% of the total of 196 micro firms have 'offsite working' with 14% having a written security policy and 28% not. Table 12 shows that 57% of small firms have 'offsite working' with 39% having a written security policy and 18% not. This shows an apparent size effect: the smaller the firm the less likely they are to have 'offsite working' or a written security policy.

Table 11: Written Security Policy v 'Offsite Working' v Firm Size: Micro Firms

	Offsite Working'?		
	Yes	**No**	**Total**
Yes	14%	12%	26%
No	28%	46%	74%
Total	42%	58%	100%

Written Security Policy?[11]

Table 12: Written Security Policy v 'Offsite Working' v Firm Size: Small Firms

	Offsite Working'?		
	Yes	**No**	**Total**
Yes	39%	13%	52%
No	18%	29%	48%
Total	57%	43%	100%

Written Security Policy?[12]

To view sector influences, 'written security policy' and 'offsite working' data in Table 10 is further cross-tabulated by sector and results are shown in Tables 13 & 14. However data for the 'Internet Services' and 'Media' sectors failed the Ch-square test so only data for 'Logistics' and 'Food Processing' is shown. Table 13 shows that 38% of 'Logistics' firms have 'offsite working' with 21% having a 'written security policy' and 17% not. Table 14 shows that 42% of 'Food Processing' firms have 'offsite working' with 27% having a written security policy and 17% not. So while 'Food Processing' shows significantly more firms having 'offsite working' than 'Logistics', this is not the case for use of a 'written security policy' where 'Logistics' has a slightly higher rate of adoption than 'Food Processing'.

Table 13: Written Security Policy v 'Offsite Working' v Sector: Logistics

	Offsite Working'?		
	Yes	**No**	**Total**
Yes	21%	12%	33%
No	17%	50%	67%
Total	38%	62%	100%

Written Security Policy?[13]

Table 14: Written Security Policy v 'Offsite Working' v Sector: Food Processing

	Offsite Working'?		
	Yes	**No**	**Total**
Yes	27%	17%	45%
No	15%	40%	55%
Total	42%	58%	100%

Written Security Policy?[14]

[11] Missing: 9; Chi-square significance: .041
[12] Missing: 4; Chi-square significance: .000
[13] Missing: 2; Chi-square significance: .000
[14] Missing: 6; Chi-square significance: .001

5 DISCUSSION

To give some perspective to data in the whole WestFocus sample, some analysis from the bi-annual DTI Information Security Breaches Surveys of 2004 and 2006 is included in Table 15 which shows the level of threat faced by firms working in an electronic realm. The DTI data is based on a sample of 1,001 firms of all firm sizes (i.e. including large firms) so comparison with WestFocus SME data cannot be wholly valid. Nevertheless, given the paucity of empirical data on security risks faced by small firms, the DTI data acts as a benchmark here. The evidence from these surveys highlight a relatively variegated picture of some of the threats to data security: 'virus infection and disruptive software' and 'theft and fraud involving computers' have decreased in incidence after a hiatus in 2004; 'staff misuse of information systems', and 'unauthorized access by outsiders (including hacking attempts)' increased from 2002 to 2004 but have more-or-less plateaued after this; and 'systems failure or data corruption' have increased in incidence (given there is missing data for 2002).

Table 15: Type of Security breach suffered by UK businesses in 2002, 2004 & 2006 Surveys

Type of Breach	***2002***	***2004***	***2006***
Virus infection and disruptive software	41%	50%	35%
Staff misuse of information systems	11%	22%	21%
Unauthorised access by outsiders (including hacking attempts)	14%	17%	17%
Theft or fraud involving computers	6%	11%	8%
Systems failure or data corruption	N/A	27%	29%

Source: Compilation from DTI Information Security Breaches Surveys 2004 and 2006

The DTI typology does not yield exact equivalents for WestFocus data, but two comparisons are made here as a means of exploring the data. A WestFocus rate of 8% for 'Internet fraud' is exactly the same as the 2006 DTI figure for 'Theft or fraud involving computers'. However 'Security failures / problems' at 6% in WestFocus data is significantly different from the 2006 DTI figure for the nearest equivalent term 'Systems failure or data corruption' of 29%. Whatever the quality of these comparisons, and with caution extended to the value of self-revealed data on sensitive issues such as data security, the WestFocus figures do not make a case for overbearing levels of risk faced by small firms trading online. Certainly the high levels of electronically-mediated trading evident in the WestFocus data - which chime with general year-on-year volume growth in electronically-mediated trading as a whole (Fulford and Doherty, 2003) – can be set favourably against the relatively low figures for security incidents.

Further comparison between the two sets of data can be made in terms of 'security policy' and 'security training'. A figure of 40% is shared by WestFocus 'written security policy' data and the DTI 'formally defined and documented information security policy' data (2006). However, given that the 'large firms' component for the DTI finding is noted as 73%, the true figure for SME security policy in the DTI data must be lower than 40%. In terms of training WestFocus data shows a figure of 53% for the 'training for awareness of IT security issues' while DTI figures show that 35% of the sample overall undertake 'training and presentations' as one means by which firms 'make their staff aware of their obligations regarding security issues' (DTI, 2006). Further, a DTI figure of 40% for large firms implies that the figure for SMEs in the DTI sample must be lower than 35%. Accepting the inherent limitations of both of these comparisons, this analysis again reflects favourably on the WestFocus sample.

From a technological perspective, the use of Internet-related technologies found in this study shows that a basic electronic communications infrastructure (composed of Internet, email, firewalls and anti-virus software) is in place for the WestFocus sample as a whole. While the almost ubiquitous use of these technologies makes sector and firm size considerations irrelevant, sector influence is evident for a subset of other technologies examined ('wireless access', 'intranet', 'extranet/EDI' and 'video/audio conferencing') which have lower general levels of take up in comparison with the 'basic infrastructure' technologies. Greatest adoption rates – by some margin – are for 'Internet Services', with a notable high of 81% for 'wireless access'. 'Broadband' bucks the adoption-by-sector trend in that 'Media' firms are its greatest adopters, but this can be tempered by the very high levels of its adoption overall. At the level of the whole sample, the relatively high levels of Internet use for commercial purposes (such as receiving payment from customers) suggest that 'networked trading' may be entrenched in places. If sector adoption behavior established for ICT holds true for commercial

uses, then assertions made by Nah *et al.* (2004) - that firms need to develop e-business processes spanning more than one organisation in order to maintain a competitive edge – would appear most keenly matched, unsurprisingly perhaps, by the 'Internet Services' sector. Some way behind in terms of technology adoption come 'Media' and 'Food Processing', with 'Logistics' as the slight laggard. The WestFocus data does not identify high relative levels of e-commerce challenges for firms in the sample as a whole. To what extent use of a such an infrastructure guarantees secure distributed working and electronically-mediated trading for firms is by definition difficult to measure, even if some general perspective on security threat has been garnered. Nevertheless the comparatively low levels of remote access accorded by the whole sample to trading partners suggests that the majority of SMEs are not ready for and/or do not have the high levels of trust necessary for the kind of integrated trading along their supply chains propounded by writers such as Straub (2002). Certainly DTI figures add a threatening backdrop in that firms that allow remote access are twice as likely to have their networks penetrated (2006).

Mirroring work on e-commerce adoption (Martin and Matlay, 2001; Simpson and Docherty, 2004), evidence was found for differences in 'offsite working' (i.e. teleworking) on the basis of sector, and for data security practices on the basis of both sector and size. In terms of sector, 'Internet Services' demonstrated greatest attention to data security risks in terms of written security policies and provision of training for IT security awareness. As with levels of technology adoption, overall the other sectors ('Food Processing', 'Media' and 'Logistics') come some way behind in these terms. A common adoption pattern for these three sectors shows that 'security training' levels were slightly greater than 'offsite working' with 'written security policy' trailing somewhat. 'Internet Services' had a slightly higher level of 'offsite working' than 'security training' to buck the trend, but the much higher levels of technology adoption and use of 'offsite working', 'written security policy' and 'security training' mark the sector out as different to the rest. Nevertheless in all four sectors, use of a formal security policy came in third place. However additional sector level data for 'Logistics' and 'Food Processing' points to further differences in behavior with 'Food Processing' firms enjoying higher levels of 'offsite working' though lower levels of formal security policy. Suggestions that 'Food Processing' firms are more promiscuous than 'Logistics' firms in security terms should be tempered however with evidence that 'Food Processing' as a sector has more awareness training on security issues for employees than 'Logistics'.

In regard to size, generally the larger the firm, the greater the levels of written security policies and training in evidence, which chimes with work on e-commerce adoption (MacGregor and Vrazalic, 2005; Levenburg, 2005; Van Beveren and Thompson, 2002). In the WestFocus data, different behavior is apparent between 'written security policy' and 'security training' by firm size. So while response rates for 'micro' and 'small' firms show higher response rates for security training than formal security policy, the converse is true for 'medium' firms where response rates for formal security policy exceed those for security training. In the absence of additional analysis using the training variable, direct comparison between 'offsite working' and 'written security policy' for 'micro' and 'small' firms shows higher proportionate use of policy by 'small' firms than 'micro' firms.

There is a trade-off between the apparent robustness of measures taken to protect data security and the ability to trade or work with information systems. Obviously a security interface that is overly robust can stymie attempts to work remotely. As Nilles (1998) argues, tongue-in-cheek, "sensitive company information is easiest to protect from outside intruders if it is kept securely locked in the company's vaulted, main office computers with no access allowed from the outside" (p. 83). In a networked electronic world of course such a stance would be untenable, with telework by definition impossible. The ability to telework at its simplest functional level requires a PC, a telephone line, an ISP (internet service provider) account and an email agent. Then, where electronic communication is restricted to email use only between remote worker and colleagues at a central location, arguably the level of controls required to handle data safely would be relatively minimal, all things considered; similarly the ability to interrupt workflow when systems are offline may be relatively minimal. If on the other hand such 'offsite working' required direct access to a firm's systems by a mobile worker exploiting wireless technology, then additional controls may be required to provide a similar level of apparent data security. Such additional controls may bring in their train some greater potential to interrupt workflow. Thus drawing the balance between the robustness of a firm's security system and an ability to work or trade whilst offsite requires management consideration.

In a dynamic and fast-moving marketplace, wireless communications, for example, is noted as one technology posing threats to secure teleworking (Rikitake, 2002a). Adoption of 'wireless access' does not by definition imply 'remote' or 'offsite access' necessarily as wireless technologies such as Bluetooth are designed for short-distance transmissions amongst local devices and a teleworker is notionally some 'non-local' distance away from co-workers. Nevertheless it is possible to conjecture

scenarios in which teleworkers in the sample firms access systems remotely using wireless means. If critical and sensitive data were to be handled in these scenarios, then the 2006 DTI survey (whose limitations as a comparator for this study are noted above) might raise questions in data security terms when it observes that 60% of firms that allow remote access, and 40% of firms that allow staff to connect via public wireless (WiFi) hotspots), do not encrypt their transmissions. While technological solutions should be seen only as part of meeting challenges to data security, encryption, where desired, implies more complex data handling processes and working practices for firms, and hence higher costs. Given observations on resource constraints faced by small firms (Poon and Swatman, 1999; Levy and Powell, 2003; Simpson and Docherty, 2004; Fillis *et al*., 2004; Gupta and Hammond, 2005) the ability for firms to accommodate users whether 'onsite' or 'offsite' using fixed and mobile (wireless) modes and perhaps via a multiplicity of devices (e.g. PC, mobile phone) in an apparently secure extended electronic network may be beyond the level of skills, knowledge and financial resources that some smaller firms in the WestFocus sample possess. The fact that technology adoption patterns by the WestFocus sample as a whole are generally higher than relative levels of 'written security policy' use and 'awareness training for IT security issues', added to apparent resource constraints, may indicate that claims by Spinellis *et al.* (1999) that advanced technology outpaces the development of 'control practice and employee knowledge' have validity. Given that smaller firms are less likely to have a formal security policy than their larger equivalents, then it is possible to speculate further that smaller firms are more likely to have unsafe handling practices than larger firms.

If technology providers fail to meet the needs of firms as Nathan *et al.* (2003) imply, then there is a role for government agencies to step into the market gap to help ensure firms handle data securely safely. Martin amd Matlay (2001) however assert that 'there is an acute lack of engagement on behalf of small business owner/managers who are largely suspicious of government interference in industry'. Thus traditional business support mechanisms through which small firms can learn about security policy formation and safe data handling practice may fall short as a desired policy goal, as Simpson and Docherty (2004) intimate. The 'cat-and-mouse' struggles between those responsible for system security and those intent on exploiting security flaws, whether with criminal intent or otherwise, supports the case advocated by Standen and Sinclair-Jones (2003) for the use of 'ethical hackers' (i.e. trusted individuals and agencies who seek to test the security of systems in order to reveal security flaws to a target firm) by which firms can check their security posture. This is not a simple task given the variegation of devices and loci noted by which to access firms' systems, and the 'motivations, constraints and uncertainties' (Westhead and Storey, 1996: p.18) experienced by small firms that includes 'non-linear (and) sometimes chaotic behavior' (Fillis *et al.* 2004). Thus, amongst other enquiries, such an initiative would require answers to the following questions:

a) Can small firms afford such support, and if so, can they then be persuaded to make such an investment (especially those firms that may be in great need of such an offering but which show little inclination to seek out business support interventions)?

b) How can small firms be sure of the *bona fides* of such individuals and agencies?

c) How can small firms be persuaded that such individuals and agencies themselves are secure?

Given the existing legal and administrative burdens already felt by SMEs struggling to survive in an increasingly competitive marketplace, there may be little apparent enthusiasm for yet another state-sponsored instrument. Thus there may be a role for policy makers working with stakeholders to facilitate the development of an appropriate mechanism. Use of some form of licensed 'honest broker' that enjoyed a level of independence from government would likely be required.

6 CONCLUSION

This paper attempts to help fill a gap in the academic literature on data security issues in relation to electronically-mediated working by SMEs. Based on a telephone survey of 378 firms in West London and surrounding counties in early 2006 and managed by a WestFocus project team composed of researchers from Royal Holloway, Kingston and Brunel universities, this analysis attempts to explore technology adoption and threats to data security on the basis of the whole sample, and where possible on the basis of four industry sectors ('Media', 'Logistics', 'Internet Services' and 'Food Processing') and three firm sizes ('Micro', 'Small', and 'Medium') of SME. The small firms literature shows that data security is a subject mainly examined in combination with some other issue(s), and that there are few studies dedicated to security issues raised by telework *per se*. General findings on Internet-related technologies show that the basic infrastructure for secure distributed working and electronically-mediated trading is in place for the sample as a whole, even if the quality (or otherwise) of such an infrastructure cannot be ascertained.

Mirroring work on e-commerce adoption, evidence was found for differences in 'offsite working' on the basis of sector, and for data security practices on the basis of both sector and size. In terms of sector, 'Internet Services' demonstrated greatest attention to data security risks in terms of written security policies and provision of training for IT security awareness. Overall the other three sectors ('Food Processing', 'Media' and 'Logistics') came some way behind in these terms. Further sector behavior shows that 'Food Processing' firms appear to display different adoption behavior from the other sectors in regard to the relative balance between 'offsite working', use of a formal security policy and security training for employees. In terms of size, generally the smaller the firm, the lower the levels of written security policies and training in evidence, which chimes with work on e-commerce adoption. An apparent market failure allied with small firms' distrust of state-sponsored business support mechanisms begs for new approaches in the promotion of data security. Use of 'ethical hackers' by 'honest brokers' may be one approach deserving policy attention therefore. Nevertheless, whatever the relative merits and demerits of such a proposal, if teleworking and mobile working in general are to flourish amongst small firms, then greater research effort needs to be devoted to data security issues in the virtual domain that takes a small firm perspective.

APPENDIX 1: Selected review of studies examining ICT adoption that highlights the relative level of discussion on security issues

Author(s)	Description	Empirical Data	Security
Clear and Dickson (2005)	UK study examining how adoption of telework is influenced more by management attitudes, levels of worker autonomy and employment flexibility than technology provision	303 SME survey; 58 face-to-face interviews	Data security discussed only in terms of its being 'a major disadvantage to the adoption of telework'
Dixon *et al*. (2002)	Literature review providing a critique of research into ICT use by SMEs; examines UK policy and ICT targets; highlights UK regional and international differences in ICT adoption; maintains that influences of sector, age and firm size on ICT adoption is under-researched	Reviews papers that use empirical data but no primary empirical data	'Security/privacy issues' noted as one of a number of barriers to ICT adoption
Fillis *et al*. (2004)	UK study that examines factors promoting and inhibiting adoption of e-business; critiques stage models of adoption; findings show that sector has an important influence on e-business development	21 SMEs; 18 face-to-face interviews; 3 phone interviews	'Security issues' mentioned as a possible impediment to future business development
Gupta and Hammond (2005)	US study examining information systems (including Internet technologies) security issues for 'small businesses'	138 small business survey using US definition of SME (1-499 employees) though only 6 responses > 200	Identifies security risks as perceived by small business owners, security incidents experienced by the sample and measures taken to guard against security threats; findings raised doubts about the effectiveness of security measures
Levenburg (2005)	US study examining how small firms use a range of 'e-business' tools in their supply chains; finds more extensive use of ICT tools in the supply chains of 'small' and 'medium-sized' firms rather than in 'micro' firms, though when a 'micro' firm adopts 'e-SCM', 'benefits are more pronounced'; finds that 'micro' firms show different use behavior from 'small' and 'medium' firms	395 SME survey	No mention of security
Levy and Powell (2003)	UK study that critiques stage adoption models; argues for an alternative 'transporter' model which recognises the fact that at adoption behavior is contingent on perceived	12 SME case studies	Brief discussion that highlights the experience felt by one firm whose customers failed to use their web site due to a perceived security risk

	business need; highlights owner attitude as instrumental in adoption decisions; identifies sector adoption behavior of firms		
MacGregor & Vrazalic (2005)	Examines e-commerce adoption barriers amongst small firms in regions in Sweden and Australia; uses statistical methods by which to derive two fundamental factors affecting adoption: either firms find e-commerce 'too difficult,' or 'unsuitable' for their business, or both	477 small firms survey	'Security' seen as a barrier but its discussion is limited; discussed mostly in terms of its being a statistically-divergent artifact for Australian and Swedish adoption practice in the two factor model
Martin and Matlay (2001)	UK study that critiques government policy based on use of the DTI five-stage ICT adoption model (developed by Cisco); seen as deficient due to its 'one-size-fits-all' underpinning that is based on wholly linear progression and that ignores key influences such as sector, size, ethnicity, gender, human & financial resources, customer base and internationalisation	No empirical data	'Security systems' mentioned as part of a discussion on business support requirements for small firms
Poon and Swatman (1999)	Australian study that examines the benefits of 'small business Internet commerce'; strong interest in email detected in firms but almost no integration between firms' Internet use and internal systems found; highlights some sector influences	23 small firms	No mention of 'security'
Quayle (2002)	UK study that examines levels of awareness about e-commerce and levels of e-commerce adoption amongst SMEs	298 small firms survey	Mentions security in the literature review as one of a number of 'hurdles' to e-commerce adoption
Riemenschneider and McKinney (2002)	Brief article reporting on a US study examining advantages and disadvantages of e-commerce adoption by adopting and non-adopting firms	27 telephone interviews and 184 firm survey	'Lack of security regarding important information' seen as one of four reported disadvantages, and a predominant concern for non-adopters
Shiels *et al.* (2003)	UK study examining ICT adoption in firms in four sectors using an 'ICT Exploitation and Integration Model' which posits four levels of ICT sophistication: 'technical integration', 'operational integration', 'inter-organisational integration' and 'strategic integration'.	24 SME case studies	Mentions network security and security of back-ups in discussion of 'technical integration'
Simpson and Docherty (2004)	UK study examining barriers and drivers for e-commerce adoption; critical of UK business support mechanisms; argues SME distrust of government business support may allow third party vendors to exploit SME ignorance	Small number (undefined) of interviews with owner-managers	Security concerns noted as one of a number of barriers to e-commerce adoption
Spinellis *et al.* (1999)	Conceptual study that examines security requirements for the 'small enterprise' and 'home-office environments'; argues for use of risk analysis methodologies and uses two scenarios as exemplars by which to illustrate security threats; makes a series of recommendations for potential solutions to threats.	No empirical data	Focuses on security issues related to 'small enterprises' and home offices and notes that these can suffer serious security problems as they typically lack the technical expertise to create and maintain a suitable level of security. Finds that SMES and home offices face similar levels of risk.

Stockdale and Standing (2004)	Australian study that identifies SME benefits and barriers to e-commerce	No empirical data	Security not mentioned
Stockdale and Standing (2006)	Australian study examining drivers and barriers for e-commerce adoption; draws up a typology of SME adopters	Combination of secondary case study data and 'interactions' with stakeholders	'Security and worries about fraud' noted in a brief discussion on security issues
Sturgeon (1996)	US study that examines drivers for telework and the security threats and risks that it poses for firms (i.e. it does not focus on small firms *per se*), especially in terms of sensitive data. Written before wireless modes of communication became common though measures to manage risks appear valid still	Uses small number of anonymised case studies to highlight vulnerabilities	Focuses on threats to data security raised by telework under a taxonomy that includes 'disclosure', 'interruption', 'modification', 'destruction' and 'removal'; argues for risk assessment; recommends various types of measure to manage threats
Taylor and Murphy (2004)	UK study that critiques DTI adoption model echoing Martin and Matlay (2001) and argues for the use of the PITs model (Foley and Ram, 2002); discusses barriers to adoption and tries to identify factors that promote 'successful adoption of e-business technologies'	Discusses empirical data provided by other researchers	As a barrier to entry into the digital economy, notes there are perceptions of unresolved security and privacy issues which most acutely identifies online payment and which discourage small firm adoption of 'this technology' and e-business
Van Beveren and Thomson (2002)	Brief paper reporting on an Australian study that highlights firm size as a factor that influences e-commerce adoption	179 SME survey of manufacturers	No mention of 'security'

REFERENCES

Beaver, G. (2002), Small Business and Enterprise Development, Prentice Hall

Clear and Dickson (2005), Teleworking practice in small and medium-sized firms: management style and worker autonomy, New Technology, Work and Employment, Vol. 20(3), pp. 218-233

Dickson, K. and Clear, F. (2003), Transnational Report of the Qualitative Research Phase: A Comparative Analysis of Regional Findings, IST project 'eGap' (IST-2001-35179) www.egap-eu.com (accessed 10-07-06)

Dixon, T., Thompson, B. and McAllister, P. (2002), The Value of ICT for SMEs in the UK: A Critical Review of Literature, Report for the Small Business Service Research Programme, The College of Estate Management, Reading.

DTI (2003), Small Business Service Excel Tables - SME Statistics UK 2003, Table 1: UK Whole Economy, http://www.sbs.gov.uk/default.php?page=/analytical/statistics/smestats.php (accessed 10-07-06)

DTI (2004), Information Security Breaches Survey 2004 Technical Report, HMSO

DTI (2006), Information Security Breaches Survey 2006 Technical Report, HMSO

European Commission (2002), Benchmarking National and Regional E-business Policies for SMEs, final report of the Ebusiness Policy Group of the European Union, Brussels, 28 June.

Fillis, I., Johansson U. and Wagner, B. (2004), A qualitative investigation of smaller firm e-business development, Journal of Small Business and Enterprise Development, Vol. 11(3), pp. 349-361

Fulford. H. and Doherty, N (2003), The application of information security policies in large UK-based organizations: an exploratory investigation, Information Management & Computer Security, Vol. 11, No. 3, pp. 106-114

Fulton, C., Haplin, E. and Walker, S. (2001), Privacy Meets Home-based eWork, Proceedings of the Eighth International Assembly on Telework, Helsinki, September 12th-14th http://www.telework2001.fi/FultonHalpinWalker.pdf (accessed 10-07-06)

Ghosh, A. and Swaminatha, T. (2001), Software Security and Privacy Risks in Mobile E-Commerce, Communications of the ACM, Vol. 44(2), February

Gordon, G (2004) Administration and General Info FAQ. What about the security or confidentiality concerns for telecommuting? www.gilgordon.com/telecommuting/adminfaq/admin10.htm (accessed 10-07-06)

Gupta, A. and Hammond, R. (2005), Information systems security issues and decisions for small businesses. An empirical examination, Information Management & Computer Security, Vol. 13(4), pp. 297-310.

Higgins, H. (1999), Corporate system security: towards an integrated management approach, Information Management & Computer Security, Vol. 7 No. 5, pp. 217 - 222

Huws, U. and Prodo, S. (1995), Employment of homeworkers: Examples of good practice, ILO: Geneva

Illegems, V. and Verbeke, A. (2003), Moving Towards the Virtual Workplace, Edward Elgar: Cheltenham

Kuhn, D, Tracy, M. and Frankel, S. (2002), Security for Telecommuting and Broadband Communications: Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, Gaithersburg, MD

Levenberg, N. (2005), Does Size matter? Small Firms' Use of E-Business Tools in the Supply Chain, Electronic markets, Vo. 15(2), pp. 94-105

Levy, M. and Powell, P. (2003), Exploring SME Internet Adoption: Towards a Contingent Model, Electronic Markets, Vol. 13(2), pp. 173-181

Lim, V., and Teo, T. (2000), To work or not to work at home - An empirical investigation of factors affecting attitudes towards teleworking, Journal of Managerial Psychology, Vol. 15, No. 6, pp. 560-586

Lohmeyer D., Mcory, J and Pogreb, S. (2002) "Managing information security, McKinsey Quarterly.

Lundegaard, K (1997). Telecommuting issues. What to consider if you're an employer, Washington Business Journal, July 7th. http://Washington.bizjournals.com/Washington/stories/1997/07/07/focus2.html (accessed 10-07-06)

Martin, L. and Matlay, H. (2001), "Blanket" Approaches to Promoting ICT in Small Firms: Some Lessons from the DTI Adoption Model in the UK, Internet Research: Electronic Networking Applications and Policy, Vol. 11, No. 5, pp. 399-410

MacGregor, R. and Vrazalic, L. (2005), A basic model of electronic commerce adoption barriers. A study of regional small businesses in Sweden and Australia, Journal of Small Business and Enterprise Development, Vol. 12, No. 4 pp. 510-527

McLeod, R., and Schell, G. (1997), Management Information Systems, Prentice-Hall

Nah, F., Rosemann, M., and Watson, E. (2004), E-Business Process Management, Business Process Management Journal, 10(1)

Nathan, M., Carpenter, G., Roberts, S., Ferguson, L. and Knox, H. (2003), Getting by, Not Getting On: Technology in UK Workplaces, The Work Foundation: London

Nilles, J. (1998), Managing Telework, Strategies for Managing the Virtual Workforce, John Wiley: New York

NISS (National Information Systems Security) (1992), INFOSEC Glossary, NSTISSI No. 4009, June 5, 1992, National Security Telecommunications and Information Systems Security Committee, NSA, Ft. Meade, MD 20755-6000

Poon S. and Swatman P. (1999), An Exploratory Study of Small Business Internet Commerce Issues, Information and Management, Vol. 35, No. 1, pp. 9-18.

Quayle, M. (2004) E-commerce the challenge for UK SMEs in the Twenty-First Century, Journal of Operations and Production Management. Vol. 22, No. 10, pp. 1148-1161

Ratnasingham, P. (1998), Trust in web-based electronic commerce security, Information Management & Computer Security, Vol. 6, No. 4, pp. 162-166

Reimenscheider, C. and McKinney, V. (2001), Assessing Beliefs in Small Business Adopters and Non-Adopters of Web-Based E-Commerce, Journal of Computer Information Systems, Vol. 42, No. 2, pp. 101-107

Reuvid, J. (2004). The secure online business handbook: E-commerce, IT functionality and business continuity (2nd ed.), Kogan Page: London.

Rikitake, K., Kikuchi, T., Nagata, H., Hamai, T. and Asami, T (2001), Security Issues on Home Teleworking over Internet, IEICE Technical Report IA2001-20, Vol. 101, No. 440, pp. 9-16

Rikitake, K., Kikuchi, T., Nagata, H., Hamai, T. and Asami, T (2002a), Secure Teleworking over Wireless Internet, IEICE General Conference Symposium, SB-12-3, IEICE

Rikitake, K., Kikuchi, T., Nagata, H., Hamai, T. and Asami, T. (2002b), Secure Gateway System Design for Home Teleworking, IPSJ SIG Notes 2002-CSEC-17, Vol. 2002, pp. 1-6

Schneier, B (2000), Secrets and Lies: Digital Security in a Networked World, John Wiley: New York

Schneier, B (2003), Beyond Fear: Thinking Sensibly about Security in an Uncertain World, Springer-Verlag

Shiels, H., McIvor, R. and O'Reilly, D. (2003), Understanding the implications of ICT adoption: insights from SMEs, Logistics Information Management, Vol. 16(5), pp. 312 – 326

Simpson, M. and Docherty, A. (2004), E-commerce adoption support and advice for UK SMEs, Journal of Small Business and Enterprise Development, Vol. 11, No. 3, pp. 315-328

Smith, A. and Rupp, W. (2002), Issues in cybersecurity; understanding the potential risks associated with hackers/crackers, Information Management & Computer Security, Vol. 10(4), pp. 178-183

Smith, G. (1998), An Electronic Pearl harbour? Not Likely!, Issues on Science and Technology, 15, pp. 68-73

Spinellis, D., Kokolakis, S., Gritzalis, S. (1999), Security requirements, risks and recommendations for small enterprise and home-office environments, Information Management and Computer Security, Vol. 7 No. 3, pp. 121-128

Standen, P. and Sinclair-Jones, J. (2003) eWork in Regional Australia, Industries Research and Development Corporation, Australian Government. http://www.rirdc.gov.au/reports/HCC/04-045.pdf (Accessed 10-07-06)

Stockdale, R. and Standing, C. (2004), Benefits and barriers of electronic marketplace participation: an SME perspective, Journal of Enterprise Information Management, Vol. 17(4), pp. 301-311

Stockdale, R. and Standing, C. (2006), A Classification Model to Support E-Commerce Adoption Initiatives, Journal of Small Business Enterprise and Development, Vol. 13(3), pp. 381-394

Straub, D (2002), Foundations of Net-Enhanced Organizations , Wiley

Sturgeon, A. (1996). Telework: threats, risks and solutions, Information Management and Computer Security, 4(2), 27-38.

Taylor, M and Murphy, A (2004), SMEs and e-business, Journal of Small Business and Enterprise Development, Vol. 11, No. 3, pp. 280-289

Tran, E. and Atkinson M. (2002), Security of personal data across national borders, Information Management & Computer Security, Vol. 10, No. 5, pp. 237-241

Tremblay, D (2002), Balancing work and family with telework? Organizational issues and challenges for women and managers, Women in Management Review, Vol. 17, No. 3-4, pp.

UK online for business (2000), Working Anywhere. Explaining telework for individuals and organisations, DfEE / DTI / DETR

Van Beveren, J. and Thompson, H. (2002), The use of electronic commerce by SMEs in Victoria, Australia, Journal of Small Business Management, Vol. 40, No. 3, pp. 250-253

Walden, I. (2005), Crime and Security in Cyberspace, Cambridge Review of International Affairs, Vol. 18, No. 1, pp. 51-68

Watson, R., Berthon, P., Pitt, L. and Kinkhan, G. (2000), Electronic Commerce: The Strategic Perspective, Dryden Press: Orlando, Florida

Westhead, P. and Storey, D. (1996), Management Training and Small Firm Performance: Why is the Link so Weak?, International Small Business Journal, Vol. 14, No. 4, pp. 13-24