

Telecommuting – In this virtual world, what is holding it back ?

Whiteman, S. A. and Dick, G. N
University of New South Wales

Abstract: Telecommuting is a work method that is relevant to the Australian knowledge worker and technologist alike. For decades, commentators have extolled the benefits and growth potential of telecommuting in Australia. The high adoption rates once forecast have not been realised and the study reported here seeks to increase understanding of the inhibiting factors. This paper addresses three issues in an effort to establish whether they are indeed inhibiting factors in the telecommuting adoption decision and if so, to what extent. These three issues are employee privacy, computer security and employee-employer trust. The analysis has prioritised and ranked the most important management concerns. Further analysis was then applied to test the relationships between the three concepts and the inhibition of telecommuting. The results indicate that four key issues are significantly and highly correlated to the decision to inhibit telecommuting.

Keywords: telecommuting, trust, privacy, security

Introduction

Telecommuting has a plethora of acknowledged advantages, if it is implemented in the appropriate business environment. These advantages can offer organisations, among other benefits, increased productivity [1] and the ability to recruit and retain the best employees [2]. Although telecommuting only affects a minor percentage of the Australian workforce, in an age of laptop computers, remote network access, and emerging wireless technologies, telecommuting is a work method that is expanding and growing in importance in the Australian workplace and information technology landscape.

Although numerous experts claimed that telecommuting was ‘the future of work’ arrangement, e.g. [3], the adoption of telecommuting practices has been slower than forecasted [4]. The contributing factors to this slow adoption have previously been identified as a lack of organisational awareness, and management inertia [5]. These have prevented most organisations from realising the many potential benefits of successfully deployed telecommuting programs.

Australia, along with many other countries, has been slow in adopting telecommuting arrangements. Australia has a high concentration of urbanised population in coastal cities and a high percentage of its well educated workforce is engaged in the services sector. The Australian environment is suitable to the use of telecommuting arrangements, however, has lagged other OECD nations in the level of adoption of telecommuting for some time [6].

With the advent of the wireless phenomenon, work conducted in wireless cafes, and airport hotspots is defined as telecommuting [7]. Such technologies are facilitating the growth and increasing the attractiveness of telecommuting to a new generation of knowledge workers.

With the availability of broadband technologies to homes in most industrialised countries, telecommuting is now, more than ever, an accessible and feasible work method for greater numbers of knowledge workers. For example in the past, professionals, such as architects, could not efficiently work from home using the available technologies (narrowband). Greater access to new technologies in the home is increasing the relevance of telecommuting as a work practice with potential to grow.

Telecommuting researchers have determined that management concerns are a significant constraint on the decision to adopt telecommuting [8]. This literature provided evidence and grounding that management

concerns surrounding computer security, information privacy and employer-employee trust could be determinants in the decision to inhibit telecommuting.

Telecommuting trust researchers Harrington and Ruppel have called for additional research to be conducted in different contexts [9], and this research answers that call by reviewing the operationalisation of the trust constructs in the context of an Australian empirical study. The Harrington and Ruppel study was conducted only on information technology managers, whereas this research reports the opinions of managers from many functional departments.

1. Background

Management resistance to telecommuting adoption remains an issue in the Australian workplace. An Australian Bureau of Statistics [10] report highlighted that Australian managers remain hesitant about the adoption of telecommuting of subordinates. Employers not allowing telecommuting was cited as the second most common reason (14% of respondents) for employed persons not telecommuting more often (after the work not being suitable).

1.1. Security

Telecommuting security is cited in the literature as a known managerial constraint to the adoption, diffusion and success of telecommuting within organisations [11]. Gray et al [12] were one of the first telecommuting publications to discuss security in any detailed way. However, Gray et al do not analyse security in terms of whether it is a determinant factor of management's decision, instead security is treated as a practical consideration, along with 'technology', to be addressed once a person is approved to telecommute. More recent publications do, however, address security as a risk that is a part of every telecommuting arrangement.

For the purposes of this paper, 'telecommuting security' covers both information security and physical security. The issue of information security includes data within the telecommuter's home, and the information that is being transmitted between it and a corporate network. Physical security includes telecommuter's hardware devices, and includes the possibility of theft and damage thereof.

A number of information security issues have been identified in the literature. A large proportion of information security issues are raised in the popular press, as the very subject matter of telecommuter computer and information security is a relatively new concept in academic literature. That said, an example of an information security issue covered in the literature is the complacency of management to rely upon corporate firewalls to nullify the risk of unauthorised remote access [13].

Another information security issue addressed in the literature is a deliberate interception of company data by competitors or any other unauthorised person [1]. In the hacker community, the type of attack whereby a virtual private network in use by a telecommuter becomes the platform facilitating an entry point, and the ability to compromise a corporate network is termed a 'U-turn' attack [14]. An Australian study found that there is a perception in the minds of managers that allowing employees to access a corporate database from a remote site, increases the risks of disclosure of commercial-in-confidence materials [15]. This research focuses on testing whether information interception has a relationship with the inhibition of telecommuting.

Another issue, or risk, of telecommuting identified by the literature is the theft of equipment from a telecommuter's home [16]. An example used in the popular press of the high incidence of laptop theft, is in July of 2001, when the FBI announced that 184 of its 13,000 laptops were missing, and more alarmingly, that 13 of them had been stolen [17]. In an Australian study, results suggested that safeguarding of corporate assets in the home is a concern to management [15]. The issue of physical security involves a number of facets, and therefore a number of questionnaire items were included to canvas the various aspects.

Orlikowski and Barley [18] claim that there is a distinct lack of research of the impact of new technologies on the adoption rate of telecommuting. This study goes some way to addressing the issue by including a number of questionnaire items that aim to ascertain the relationship between telecommuting and the security authentication devices, security tokens, and password protection.

Although not covered in the literature to the extent of other telecommuter security issues, security and legal liability issue were deemed relevant for this research, as they are likely to impact management

attitudes towards telecommuting. Telecommuting can present legal issues, for example a scenario where family members use a corporate PC to download sexually explicit or illegal materials. This is not a completely fictional scenario, in California, an employee used corporate hardware to access illicit material in his home and was dismissed under Californian law (*Insurance Services Corp. v. Superior Court of Los Angeles County*, 2002). Another physical security issue that this research seeks to understand is the security and liability issue of viruses or worms entering a corporate network via a telecommuters remote access point.

1.2. Privacy

Surveillance and monitoring is a method for the manager to maintain control over subordinates, through the collection of objective data on employees, rather than relying on personal relationships [19]. Computer based performance monitoring allows managers to monitor telecommuting employees in great detail, and the availability of technology based access may even lead decision makers to seek out information they would not have asked for in person [20].

Both physical and information privacy are telecommuter related issues, as the line between work and home blurs. Employer management boundaries are untested and it is unknown, for example, whether an employer can legally enter an employee's home to inspect workplace safety or security measures.

The issue of telecommuter privacy is a trade-off between the legitimate needs of an organisation, and the fundamental right of an individual to privacy. Spinello [21] argues that if a corporation has legitimate suspicions that an employee is using its systems for untoward or frivolous reasons, then the corporation should investigate. However, when there is no such suspicion, the possibility of the abuse of corporate systems should not outweigh the reasonable expectation of employees to be trusted by their employer. Employee privacy is related to the issue of the loss of direct control that many managers are uncomfortable relinquishing [22].

1.3. Trust

The concept of trust is one that has recently received much attention in the information systems and decision science arena, and researchers are endeavouring to model all possible dimensions of trust [23]. This study looks specifically at employee-employer trust in the context of a telecommuting adoption decision.

The telecommuting literature suggests that a lack of trust is a management attitude that influences telecommuting because it is believed that managers cannot manage what they cannot see, or that out of sight, employees will engage in opportunistic behaviour [9, 24, 25, 26]. It is well documented in the telecommuting literature that the supervision method used by management has a relationship with the adoption of telecommuting. The vast majority of studies strongly correlate visual management, otherwise known as traditional management with the inhibition and failure of telecommuting initiatives.

The ability to see, or inspect workers is used by managers as the input to the productivity equation [27]. Thus traditional management see the need for direct personal control of employees because of a lack of trust in the employees and the assumption that employees need to be motivated by an office environment [28]. More importantly, management opposition to telecommuting is believed to be based on this more traditional lack of trust of employees [9, 24, 26, 29]. Trust of the employee also extends to the custodianship of organisational assets, such as laptop computers.

There is little research on the impact of managers' trust of potential and existing telecommuters, and its effect on the decision to allow telecommuting [9]. Perin [27] interviewed professionals and their managers to understand why, although organisations would allow telecommuting, the professional employees were not participating in it. While the focus of the study was on the professionals themselves, Perin found that the need for employee presence, visibility of hours worked, and punctuality lead to distrust on the part of management and the reluctance of the interviewed professionals to participate in telecommuting options [9].

1.4. Objective

The objective of this study was to firstly rank the importance of the three concepts of security, privacy and trust, and during this analysis to gain an understanding of what issues have highest importance to of managers; then to assess whether these factors were inhibiting the take-up of telecommuting.

2. Methodology

A survey instrument was developed and piloted in a small-medium sized organisation, and the instrument was refined. The improved instrument was then piloted in the main study organisation and was used for “test-retest” purposes. The modified (and final) survey instrument was then distributed to managers and employees in the main study organisation. Face validity was established in the demographic questions by adapting relevant demographic questions from a validated telecommuter study by Belanger [30]. Belanger based her demographic questions on research by earlier telecommuting researchers who identified particular demographic groups as having an impact on data results, for example, job title. Face validity was further established by using expert researchers as evaluators, as the more experts who agree that the questionnaire does indeed measure what it claims to measure, the greater the level of face validity [31]. A further advantage of conducting face validity tests with an expert sample is that they are able to critique some of the external validity issues associated with the questions presented [32].

The main study was completed in a large Australian telecommunications organisation. The researcher was placed at the organisation for a six month period, whereby, access to research subjects was facilitated. Working within the organisation which is the sole subject of empirical research has certain limitations (see later).

Research participants were all Sydney based knowledge workers and were full-time employees of the main study organisation who performed roles in a variety of areas including IT, marketing, sales, operations and legal. Managers and employees across all functional departments in the organisation were randomly selected. The randomisation was achieved by picking names from organisational charts. The survey distribution method was hand-delivery, as pilot studies had illustrated that this method achieved high response rates. The response rate for the main study was 69% (n = 86).

Cronbach alpha scores for the three constructs of security, privacy and trust were all above .6, so can be considered acceptable [33]. The procedures followed give considerable support to the external validity of the findings from this study. These include the selection of respondents from the main study organisation, almost all of whom were knowledge workers engaged in full-time employment; the randomisation of survey distribution; the selection of respondents from a wide range of functional departments, and performing jobs where some form of telecommuting was possible; a high response rate for survey-type research; potential survey respondents had no obligation to their organisation, their manager, or the researcher to complete the survey; and anonymity.

3. Results

The analysis used to rank the relative importance of the three issues was the non-parametric Mann-Whitney mean rank test. The grouping variable was managers and non-managers, and the variables were the ranks given to the survey questions by the participants.

For the sample of managers, the lowest mean rank (and hence the most important issue) was trust, followed by information security, physical security and the least important issue was privacy. It is important to note that the statistical significance of the mean ranks was quite poor, hence the means ranks are not reliable and conclusions should only be drawn in general terms. .

When the questionnaire items that are most strongly correlated with the inhibition of telecommuting are singled out, we were left with four issues, all of which are statistically significant. Two of the questions are privacy related, and the remaining two questions relate to security and trust respectively. It is valuable to concatenate these issues, and measure the influence that they have on the inhibition of telecommuting. The resulting statistic would be an indication of the importance these three issues have on the decision to inhibit telecommuting.

Multiple (linear) regression was used to analyse these four issues against inhibition – the resulting R^2 score is 0.38. This R squared score is significant to the 0.001 level, and has a high F score (6.13), both of which indicate a high level of statistical significance. This result indicates that 38% of movement in the decision to inhibit telecommuting can be explained by movement in the four key issues - which relate back to security, privacy and trust. This is a high level of correlation, and the result indicates the key importance of the four issues, namely:

- The availability of computer authentication tools for telecommuters, such as tokens [computer security]
- The unauthorised use of personal information that relates to telecommuters [employee privacy]
- The ability and right of management to control and monitor telecommuters via hardware, and its contents [employee privacy]
- The level of trust management have that their employees have an adequate level of expertise to cope with telecommuting and new technologies [employee-employer trust]

This finding indicates the strength of the relationship between the four key issues and managers' inhibition propensity. It also demonstrates the four key issues are indeed significant determinants in the telecommuting inhibition decision.

4. Discussion

Managers regard the complex issue of trust as the most important concept. And, while regression analysis showed that the three issues have a poor level of statistical significance when they are treated as individual and independent concepts, when the analysis was more comprehensive, and addressed each questionnaire item individually, some interesting results emerged.

First, it was found that a number of key issues existed within each concept. These key issues were both statistically significant, but also statistically important to (a) the comfort level of telecommuters and their managers, and also to (b) managers' decision to inhibit telecommuting.

The multiple regression revealed perhaps the most important finding of this research - the combined importance of the key issues when they were measured against the inhibition of telecommuting. A high 38% correlation between the key issues of security, privacy and trust and telecommuting inhibition is a result which not only justifies research in this new arena, but also reinforces the importance and practical significance of the three emerging issues in the telecommuting decision.

The issues of computer security, employee privacy and employee-employer trust are emerging issues, which are growing in importance as new technologies facilitate greater use of telecommuting. These new technologies, such as broadband internet and wireless networks, introduce a new set of telecommuter security and privacy concerns that were previously of no consequence. Today, computer security and trust are major areas of information systems research, and hence are of high importance in the telecommuting area. Prominent telecommuting researchers have been calling for additional research in the area of telecommuter trust, and this study goes some way to answering such calls.

There are limitations to this work – the sample size was small, the study was conducted in just one organisation, the researcher was placed there, there are the normal concerns with survey based research and the survey results are at a particular period in time.

Nevertheless, this empirical research contributes to the literature by increasing understanding of the Australian manager's attitudes towards inhibiting telecommuting. Through understanding management concerns around computer security, privacy and trust concerns, regulators, governments, technologists and telecommunications organisations are better able to tailor campaigns and drive adoption of telecommuting in Australia.

References

- [1] Ford, R. and Butts, M. (1991) "Is your organisation ready for Telecommuting?" SAM Advanced Management Journal 56 pp19-23.
- [2] Turban, E. and Wang, P. (1995) "Telecommuting Management: A Comprehensive Overview", Human Systems Management 14, pp.227-238.
- [3] Toffler, A. (1980) The Third Wave, London William Collins Sons & Co. Ltd.
- [4] Korzeniowski, P.(1997) "The telecommuting dilemma", Business Communications Review, 27, pp29-32.
- [5] Fritz, Higa and Narasimhan (1994) "Telework: Exploring the borderless office" Proceedings of the 27th annual Hawaii international conference on Systems Science.
- [6] Wood, J. (1992) "Telecommuting: a New Challenge for Human Resource Managers" Management Update April/May pp8-9

- [7] Driscoll, E. B. Jr., (2002) "Wanna be wireless?" *Planning* 68 (9) September, pp30-33.
- [8] Mokhtarian, P. L. and Salomon, I. (1996) "Modelling the desire to telecommute: the importance of attitudinal factors in behavioural models" *Transportation Research A*, 31 (1), pp. 35-50.
- [9] Harrington, S. and Ruppel, C. (1999) "Telecommuting: A Test of Trust, Competing Values, and Relative Advantage" *IEEE Transactions on Professional Communication*, 42 (4) December, pp 223-239.
- [10] Australian Bureau of Statistics (2001) "Teleworking, New South Wales" 1373.1, October.
- [11] Ellis, T. and Webster, R. (1997) "Information Systems Managers' Perceptions of the Advantages and Disadvantages of Telecommuting: A Multivariate Analysis" *IEEE* 1060-3425, pp. 94-98.
- [12] Gray, Hodson and Gordon (1993) *Teleworking Explained*, John Wiley & Sons Ltd.
- [13] Goslar, M. (2000) "The new e-security frontier" *Informationweek*, July 10.
- [14] ESC security, (2000) "Yesterday's Conventional Threats", in PowerPoint presentation titled, ESC-Security products, slide number nine. URL: www.esc.com.
- [15] Garner, G. and Dick, G. (1997) "Telecommuting: A Managerial Perspective" *Multiconference on Systemic, Cybernetics and Informatics*, Caracas, Venezuela, July, pp 374-381.
- [16] Zbar, J. (2000) "Working home alone? How's the security?" *Network World*, November 13, 2000.
- [17] Kliner, M. (2001) "Routers, firewalls and loading devices help telecommuters and road warriors secure their data and computers" *Government Computer News* 20 (27) pp58-.
- [18] Orlikowski and Barley (2001) "Executive Overview; Technology and Institutions: What can Research on Information Technology and Research on Organizations Learn from each other?" *MIS Quarterly*, 25 (2), June, pp145-165.
- [19] Fairweather, B. (1999) "Surveillance in employment: The case of Teleworking" *Journal of Business Ethics* 22 (1), pp 39-49.
- [20] Lally, L. (1996) "Privacy versus Accessibility: The Impact of Situationally Conditioned Belief" *Journal of Business Ethics* 15, pp 1221-1226.
- [21] Spinello, R. (1997) "The Case for E-mail Privacy" *The second annual ethics and technology conference*, Chicago, June.
- [22] Dombrow, J. (1998) "Electronic Communications and the law: Help or Hindrance to Telecommuting?" *Federal Communications Law Journal* 50 (3) pp 685-709.
- [23] Jones, A. J. I. (2002) "On the concept of trust" *Decision Support Systems* 942, March.
- [24] Christensen, K. (1992) "Managing invisible employees: How to meet the telecommuting challenge" *Employee Relations Today*, Summer pp. 133-143
- [25] Bresnahan, J. (1998) "Why telework?", *CIO* 11 (7), pp 28-37.
- [26] Handy, C. "Trust and the Virtual Organisation" (1995) *Harvard Business Review* 73 (3), pp 40-50.
- [27] Perin, C. (1991) "The Moral Fabric of the Office: Panopticon Discourse and Schedule Flexibilities", in *Research in the Sociology of Organisation*, P.Tolbert and S.R. Bartley (eds.). JAI Press, Greenwich, CT, 1991.
- [28] Creed, W. and Miles, R. (1996) "Trust in organisations: A conceptual framework linking organisational forms, managerial philosophies, and the opportunity costs of controls" in *Trust in Organisations: Frontiers of Theory and Research*, T.R.Tyler and R. M. Kramer, Eds. Thousand Oaks, CA: Sage, pp 16-38.
- [29] Reinsch, N. (1997) "Relationships between telecommuting workers and their managers: An exploratory study" *Journal of Business Communication* 34 (4) pp 343-369.
- [30] Belanger, F. (1999) "Workers' propensity to telecommute: An empirical study" *Information and Management* 35 pp 139-153.
- [31] Neuman (2000) *Social Research Methods: Qualitative and quantitative approaches* London, Sage.
- [32] Trochim, W. K. (2001) the validity page of the Cornell university research methods knowledge base, URL: <http://trochim.human.cornell.edu/tutorial/maldon/validity.htm>
- [33] DeVellis, R.F. (1991) *Scale Development - Theory and Applications*, Newbury Park, CA.