Security Risks in Teleworking:

A Review and Analysis

Huiyi Yang, Chaofan Zheng, Lika Zhu, Fei Chen, Yumin Zhao, Manjeera Valluri

Department of Computing and Information Systems

University of Melbourne

Abstract

Teleworking as an innovative working practice attracts organizations to apply it throughout whole organizations, with providing plenty of benefits. However, the related information security risks generated in teleworking threaten organizations to implement it. This paper aims to ascertain information security risks arising from teleworking based on literature. The contributions of this paper are addressing most challenging security risks that existed in teleworking for companies to be concerned, providing security controls for avoiding these mentionable risks that are identified, generally discussing which component of the risks are more crucial for the risk control, and indicating intangible security risks not mentioned in literature. These risks are aligned with teleworking business goals.

Keywords: Teleworking, Telecommuting, Security risks, Control, Information Security, Teleworkers.

Introduction

Due to high-capacity broadband networking applied by organizations, teleworking, or known as telecommuting, defined as employees and contractors' ability to implement works through using information and telecommunication technologies from locations other than organization's facilities, becomes a more attractive prospect for enterprises (Scarfone, Hoffman & Souppaya, 2009). Teleworking creates benefits for organizations indicated in literature, in acting as a motivator, morale booster, and environmentally friendly alternative to ensure companies' success in conquering virtual workplace (Godlove, 2012). However, teleworking performance would also generate an emergence of new information security risks, threatening organizations to implement teleworking, which obstructs companies to absorb benefits generated by teleworking. Literature evidence demonstrated that most employers agreed that security concerns and the effect of teleworking on profits were reasons to deter implementation of teleworking programs within organizations (Blackwell & Demerath, 2002). It is very important for companies to be aware significance of teleworking performance by better understanding how to mitigate those risks, in order to acquire benefits from teleworking to achieve success in business.

For the preceding reasons the research questions in this paper are:

1. What are the security risks that may arise in teleworking?
2. What are the related triggers?
3. How to control these risks?

This paper established a comprehensive literature review which defined the most common definition of teleworking agreed in literature, identified three information security risks existed in teleworking implementation including disclosure of data, modification of data and destruction of data required to be aware by organizations, indicated triggers that caused these risks and provided risk controls for companies to mitigate security risks. Methodology section pointed out how authors constructed literature review. A further discussion was conducted to align teleworking risks management with its business goals and attempted to generally discuss which risks were more crucial for the risk control. Arguments about intangible risks indicated security risks which had not been mentioned in the literature review. This paper also exposed limitations in literature review study and addressed future directions for the research of security risks generated in teleworking performance.

Literature Review

Teleworking

There was a consistency in using both "teleworking" and "telecommuting" as interchangeable terms for telework, which had been exposed in most literature. However, there had been discovered a low degree of consensus in definition of teleworking. There were two distinguished approaches towards the definition of teleworking, which contained location of teleworkers and utilization of information technologies and telecommunications addressed in the literature. In this perspective the main focus is on location where employees worked in remote areas were away from their traditional office where remains worked (Montreuil &Lippel 2003). Shin, Sheng &Higa (2000) supplemented these remote sites could be home, non-traditional satellite offices, telecottages and neighbourhood offices etc. The second perspective stressed on using computing and telecommunications as fundamental working tools for teleworkers, in order to achieve data transmission connection (Pulido & López 2005). Overmyer (2011) also addressed that teleworking appeared with facilitation and aid from information and telecommunication technologies, no matter work was done on part-time or full-time manner.

According to the vast majority of literature, a commonly agreed definition of teleworking should involve both perspectives mentioned above. The defined definition of teleworking was:

"Teleworking, also known as telecommuting, involves working away from the traditional office using computers and telecommunication facilities to maintain a link to the office" (Bélanger & Allport 2008, p. 102).

This widespread definition of teleworking was also founded in other literature, including Ruppel & Harrington (1995), Gupta, Karimi & Somers (2000), Blackwell & Demerath (2002), Bailey & Kurland (2002), and Greenhill & Wilson (2006) exhibited in the table below. This paper adopted this broadly accepted definition of teleworking for further research. In addition, this paper also viewed teleworking in three types, which were addressed in Pe´rez et al (2005). The three types of teleworking were home-based teleworking which referred to work generated at home, mobile teleworking which referred to work based on movement and utilization of communication technologies from varied sites containing plane or hotel etc, and telecenters which referred to work created in both outside the home and away from traditional office.

Literature	Definition of Teleworking
Ruppel & Harrington 1995, p. 88	"Telework, sometimes called telecommuting, combines the use of electronic equipment with a communication link to the employer to enable information workers to work at sites independent of the employer's location."
Gupta, Karimi & Somers 2000, p. 27	"Work carried out at home or at an office close to home (remote from central offices or production facilities) where the worker has no personal contact with co-workers but is able to communicate with them and perform work-related tasks using computer and communication technologies."
Blackwell & Demerath 2002, p. 76	"Working at one's home or another location where employees use computers and communication technology to communicate with the main office, supervisors, co-workers, and customers."
Bailey & Kurland 2002, p. 384	"Working outside the conventional workplace and communicating with it by way of telecommunications or computer-based technology."
Greenhill & Wilson 2006, p. 381	"Work that is carried out at a distance from the core organization through the medium of ICTs."

Security Risks in Teleworking

Risk is defined as "an asset that has a vulnerability that can be exploited by a threat, measured in terms of consequence and likelihood" (HB 231, 2004). Compared with working in the organizations, telework can lead to novel and different vulnerabilities. They will further cause a series of security risk problems. Clear and Dickson (2005), and Illegems and Verbeke (2003) indicated that risks to data security were a main challenge and issue faced by teleworking adoption. Fulton et al. (2001) also mentioned that ‘home-based e-work’ would be result in data security risks that include disclosure, modification and destruction.

Disclosure of data

Spinellis et al. (1999) pointed out that one significant risk in the scenario of telework is unauthorized disclosure. Moreover, Zernand (2003) also mentioned that in telework, the risk of information being leaked to the wrong individuals will be increased. Disclosure of data often occurs through three paths. Firstly, the employee’s family or other guests use the computer and access the data. Secondly, the hardcopy of sensitive information is misplaced or thieved. Thirdly, the information is intercepted during the transmission and unprotected communication channel (Sturgeon, 1996, and Ernst and Young, 2008).

Modification of data

The communications on external network will be susceptible to modification (Kent et al., 2009). Sturgeon (1996) described modification as the mischievous changes of information inadvertent or deliberately, which will be result in the loss of information integrity. Moreover, modification also may happens when computer having system errors. Once the information is modified, it may cause heavy financial losses (Spinellis et al., 1999).

Destruction of data

Destruction of data is another risk in telework, which means the loss of access to data or availability of data (Sturgeon, 1996). The environment of telework is uncertain and may not suitable (Pyöriä, 2011). The natural disaster such as earthquake, flood and fire will destroy the computers and devices and lead to the destruction of data. Additionally, the data access by strangers and other human factors can cause the interruption and destruction of data.

Besides the risk to data security, telework also will increase the possibilities of hacking and physical thefts (Juline et al., 2001 , and Iscan and Naktiyok, 2004). In the survey from Ernst and Young (2008), it was pointed out that physical loss and theft of information and devices was one of the risks faced by teleworking.

Triggers of the Risks in Teleworking

The following categories, which are concluded by Surgeon (1996), may be the triggers of these information security risks. They have been divided into three categories 1) personnel security issues, 2) physical security issues, and 3) administrative security issues.

Firstly, a good self-discipline is necessary for every employee. However, many teleworkers lack the sense of responsibility to follow the principles of management objectives, and they can easily endanger the success of teleworking (Zernand, 2003). For instance, many teleworkers will change the company's security settings to unlock and browse the restrict websites, they do it because they want to browse these sites, without considering the company's policies, and they always on links increase risks (Rikitake et al, 2001). Although people have signed the non-disclosure agreement without updating, the significant information or data may be disclosure by the person who is possibly for financial reasons (Sturgeon, 1996). Moreover, in the distributed environment, it is difficult to avoid BYOD. Teleworkers would use their own mobile device, and it adds risks to the information security. The PC-based systems cannot provide adequate services, as they are not designed for professional use in open environments, especially in small companies and home-offices (Spinellis, Kokolakis & Gritzalis, 1999).

Secondly, in terms of physical security, other people will easily access the computers if a employee goes outside without locking the door or device on the PC. There are vulnerabilities to the threat of disclosure and modification by accident: the threat of interruption and destruction by natural causes or by accident, also the threat of removal by theft (Sturgeon, 1996). In addition, telecommuters of small enterprises will store their data in cloud and using WIFI, wireless Internet connections is common and unsecure, it will give more opportunities for hackers of accessing the system through Internet connection and viruses may be introduced via Internet connection or diskettes used by others in the house (Sturgeon, 1996 and Ernst & Young, 2008). Moreover, telework devices are not as secure as organizational devices. Another one is the external network and communication channels of telework are not as secure as internal network, which is in the control of organization (Sturgeon, 1996, and Ernst and Young, 2008).

Finally, the vulnerability of administrative security mentioned that companies' policies were fragmented and they were incapable of preventing sensitive data or information, on the other hand, organizations do not have adequate policies and procedures to keep personal data from leaving the building (Joice, 2007, Ernst & Young, 2008, and Sturgeon, 1996).

Risk Control of Teleworking

The security risks on telecommuting will influence the effectiveness and capability of the work. The disclosure, modification and interruption of information may cause huge loss of organizations. Therefore, it is essential to improve the security of assets and information, making sure the confidentiality, integrity and availability of data. The previous studies and research proposed some solutions to maintain the security, such as setting up formal policies, developing trainings, encrypting data, backing up data, securing telework devices and communication channel, and authorizing access (Ernst and Yong, 2008, and Kent et al., 2009).

Firstly, it is necessary to develop proper policy, because "a policy is the start of security management" (Huong Ngo, 1999). In the research of Kent et al. (2009), it also stated that the organization should have proper policy to limit the application installing, encrypt data and backing up data on the telework devices. Ernst and Yong (2008, p.4) also suggested the organizations to use "a data classification policy to guide their data protection operations".

Secondly, security training is another important measure to ensure the information security in the scenario of telework (Joice, 2007, and Huws and Podro, 1995). In the research of Sturgeon (1996), it also emphasized the importance of training to improve the employees' awareness of security. Moreover, Kent et al. (2009) pointed out the lack of staffs' awareness of threats was one of the reasons leading to the failure of maintaining telework security. Therefore, developing training is a key component for solving and reducing risk problems.

Furthermore, the encryption was crucial to information security including email encryption, file encryption and disk encryption (Pyöriä, 2011 and Kent et al., 2009), which can be efficiently prevent the disclosure and modification of data (Ernst and Young, 2008). Additionally, to ensure the availability of data, back-ups are recommended by Huws and Podro (1995) and Shiels et al. (2003) in their research.

Finally, securing telework devices and communication channel can be an effective solution (Kent et al., 2009, and Ernst and Young, 2008), such as using pass words to authorize access, adopting virtual privacy networks (VPN) to improve the security of communication channel (Ernst and Young, 2008), or limiting the networking capabilities of consumer devices (Kent et al., 2009).

Methodology

The search of literature was conducted to understand the definition of teleworking, explore the security risks in teleworking and look for methodologies of risk control in teleworking and determine the most important component for telecommuting information security. Authors searched the teleworking database and Information Security database from 1995 through 2012, using the combined search terms: teleworking, distributed work security, information security, and home-office security management. The research included all developed countries but was limited to those papers which published in English.

The research questions guiding the review, 40 published articles were related to the questions, 30 articles were chosen to review, which were had the primary source, published in authority journals, and up to date. They were sorted into three categories: 11 papers related to teleworking: 1995-2011, 16 papers related to security & teleworking: 1999-2012, and 4 papers related to information security:1999-2012.

Discussion

The purpose of the study was to explore the information security risks of teleworking, in order to ascertain how it might threaten enterprise benefits and how it can be controlled into risk management. Three categories of risks were identified from the literature review: 1) The teleworkers, 2) The data and information, and 3) The software, hardware and network assets. This section attempts to disuse the most crucial component for risk control in teleworking, and the security risks were aligned with the teleworking business goals.

The employees who took part in the teleworking were the core actors of the whole telecommuting procedures. Their behaviour could directly trigger the teleworking security risks through their daily manipulating IT devices, operating business processes, and administrating the related teleworking privileges. Those teleworkers, as the potential insider threat, were the most important component which was needed to be controlled and monitored.

Securing business sensitive information and resources was also an important component for risk control. The related potential risks may lead to the data stolen or data tampering from customers, and may finally result in the financial loss and losing confidence from clients. In order to control these related potential risks, it’s necessary to require teleworkers to be aware of their daily business operation and information encryption which include the email encryption, file encryption and disk encryption. Moreover, security awareness training is essential for these telecommuters, as it can assist them to make the right judgments or decision, such as to choose which location is more suitable to work and timely back-ups information.

The hardware, software and network assets will be the technical perspective of security risk. Providing technical solutions like VPN and encryption is the foundation of the security of teleworking. In a study of 143,700 of worldwide commercial hotpots in 2006, about 65.85% of computers have at least one detectable open port which has well known vulnerabilities (Chenoweth, minch &tabor 2010). This means there is high possibility of teleworkers using unsecured network and devices due to the lack of security training.

It therefore is crucial to formulate relevant security policies and security training. Timely control of these teleworkers-related risks would not only reduce the opportunities of IT risks (such as data disclosure, modification and destruction), but it also have positive influences to economically and effectively achieve the targeted business outcomes.

However, it's difficult to monitor teleworkers behaviour when they are outside of office. People are the weakest link of security in Information management (Van Kessel, 2008).

The authors' recommendations are as follows. (1) One of the ways to increase awareness of teleworkers is encouraging them into the risk assessment process because user participation increase awareness, alignment and security controls performances (Spears & Barki 2010). (2)To make the policy work effectively, the procedures should focus on the performance and attitude of teleworkers. Because one of the main reasons why many teleworkers did not completely comply with security policies is because as end users, they are more concerned about their performance than IS security so that IS security should align with end usersí¯ objectives and change through day-to-day secure computing behaviors (Guo, K, Yuan, Y, Archer, N, & Connelly, C 2011).

Argument about the Intangible Risks

Authors also consider several security risks in teleworking which has not been mentioned in the literature review.

The technology change in companies create new security risk in teleworking. For example, if a company choose to use cloud computing to store their data and sensitive information, the assess control and information manage would be in the cloud sides. This will increase the difficulty of security management which need negotiate with cloud providers. Another intangible security risk is the unhealthy teleworking culture in corporations. A healthy teleworking culture can lead to ideally benefits to companies, such as Google and Microsoft. However, many corporations do not have a fully mature teleworking culture. Telecommuters were easily being isolated from company and colleagues, and they may feel depressed or careless about their companies’ benefits, and they may not pay attention to protect their companies’ information (such as they won’t care which location are suitable for teleworking), which means that they may be more vulnerable (such as be attacked by hackers or be stolen IT device s) than they work together in an office.

Limitation and Future Direction

In this paper, the research established had its own limitations. The range of review was limited caused a small sample size for research. There was also no new data or information was collected through interview or survey of this year, therefore, the results of the review were not comprehensive and ultramodern. In addition, most of the papers were taking the perspective of small enterprises and small home offices without clearly targeting a specific industry, thus, the solutions for avoiding the security risks of teleworking might not be suitable for large organizations and all industries. Teleworking rose in the late eighty century due to its benefits generated for organizations in improving efficiency, effectiveness and convenience, which increased companies' willingness to implement it across whole organizations. However, plenty of information security risks appeared in teleworking resulted in abandoning teleworking performance by organizations. Most literature had focused on how to solve the risks referred to employees who were poorly managed and risks of ineffective internal company policies. Therefore, this paper recommended that future research could focus more on the technical aspects of information security and businesses involved all sizes from different industries. Individual countermeasures could also be presented for organizations, in order to widely use teleworking within organizations

Conclusion

Teleworking has a great contribution on organizations, while from the review of papers, it is found that teleworking may lead to the security risks of disclosure, modification and destruction of data via personnel, physical and administrative security vulnerabilities. However, these risks can be managed and some solutions have been provided in the previous studies, such as establishing formal policies, developing training, making sure the network and devices be secured and encrypting information. We consider three main components in the teleworking process in security risk 1) the teleworkers, 2) the data and information 3) the software, hardware and network assets. There are missing point in knowledge, culture, and personal network while the changes of technology create new risks and solutions for teleworking. The study of teleworking needs to be updated all the time just like other security risks.

References

2004. ‘Information security risk management guidelines: HB 231:2004 / [prepared by Committee IT/012’, *Information Systems, Security and Identification Technology, Sydney*: Standards Australia International and Standards New Zealand, 2004.

Bailey, D & Kurland, N 2002, ‘A review of telework research: findings, new directions, and lessons for the study of modern work’, *Journal of Organizational Behavior*, vol. 23, no. 4, pp. 383-400.

Bélanger, F & Allport, C 2008, ‘Collaborative technologies in knowledge telework: an exploratory study’, *Information Systems Journal*, vol. 18, no. 1, pp. 101-121.

Blackwell, J & Demerath, P 2002, ‘Telecommuting in the 21st century: benefits, issues, and a leadership model which will work’, *Journal of Leadership & Organizational Studies*, vol. 8, no. 4, pp. 75-86.

Clear, F & Dickson, K 2005, ‘Teleworking practice in small and medium-sized firms: management style and worker autonomy’, *New Technology, Work & Employment,* vol. 20**,** pp. 218-233.

Ernst and Young 2008, ‘Risk at Home: Privacy and Security in Telecommuting’, *Ernst and Young***,** pp. 1-23.

Fulton, C, Haplin, E & 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 14-07-13).

Godlove, T 2012, ‘Examination of the factors that influence teleworkers’ willingness to comply with information security guidelines’, *Information Security Journal: A Global Perspective*, vol. 21, no. 4, pp. 216 -229.

Gupta, Y, Karimi, J & Somers, T 2000, ‘A study on the usage of computer and communication technologies for telecommuting’, *IEEE Transactions on Engineering Management*, vol. 47, no. 1, pp. 26-39.

Huong Ngo, H 1999, ‘Corporate system security: towards an integrated management approach’, *Information Management and Computer Security*, vol. 7, pp. 217-221.

Huws, U & PODRO, S 1995, ‘Employment of homeworkers: Examples of good practice’, *International Labour Office*.

Illegems, V & Verbeke, A, 2003, ‘Moving towards the virtual workplace: managerial and societal perspectives on telework / Viviane Illegems’*, Alain Verbeke*, Cheltenham, UK; Northhampton, MA: Edward Elgar Pub., c2003.

Iscan, F & Naktiyok, A 2004, ‘Attitudes towards telecommuting: the Turkish case’, *Journal of Information Technology,* vol. 20**,** pp. 52-63.

Joice, W 2007, ‘Implementing Telework: The Technology Issue’, *Public Manager,* vol. 36**,** pp. 64-68.

Juline, M, Chilian, E, William, W & Joan, C 2001, ‘Employer liability for telecommuting employees’, *Cornell Hotel and Restaurant Administration Quarterly,* Vol. 42**,** pp. 48-59.

Kent, K, Hoffman, P, & Souppaya, M 2009, *Guide to enterprise telework and remote access security (draft) [electronic resource]: recommendations of the National Institute of Standards and Technology / Karen Scarfone, Paul Hoffman, Murugiah Souppaya*, Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology, [2009].

Montreuil, S & Lippel, K 2003, ‘Telework and occupational health: a Quebec empirical study and regulatory implications’, *Safety Science*, vol. 41, no. 4, pp. 339-358.

Morrow, B 2012, 'BYOD security challenges: control and protect your most sensitive data', *Network Security.* Dec2012, Vol. 2012 Issue 12, pp.5-8.

Overmyer, S 2011, ‘Implementing telework: lessons learned from four federal agencies’, *IBM Center for the Business of Government*, Washington, D.C.

Pe´rez, M, Sa´nchez, A, Carnicer, P & Jime´nez, M 2005, ‘The synergism of teleworking and information and communication technologies’, *Journal of Enterprise Information Management*, vol. 18, no. 1, pp. 95-112.

Pulido, J & López, F 2005, ‘Teleworking in the information sector in Spain’, *International Journal of Information Management*, vol. 25, no. 3, pp. 229-239.

Pyöriä, P 2011, 'Managing telework: risks, fears and rules', *Management Research Review*, 34, 4, pp. 386-399, Business Source Complete, EBSCO*host*, viewed 15 July 2013.

Ruppel, C & Harrington, S 1995, ‘Telework: an innovation nobody is getting on the bandwagon’, *Data Base for Advanced in Information Systems*, vol. 26, no. 2 & 3, pp. 87-104.

Scarfone, K, Hoffman, P & Souppaya, M 2009, *Guide to enterprise telework and remote access security: recommendations of the national institute of standards and technology*, National Institute of Standards and Technology, Gaithersburg.

Shedden, P, Scheepers, R, Smith, W & Ahmad, A 2011, 'Incorporating a knowledge perspective into security risk assessments', *The journal of information and knowledge management systems*, vol. 41 No. 2, pp. 152-166.

Shiels, H, Mcivor, R. & O'reilly, D 2003, ‘Understanding the implications of ICT adoption: insights from SMEs’, *Logistics Information Management,* vol. 16**,** pp. 312.

Shin, B, Sheng, O & Higa, K 2000, ‘Telework: existing research and future directions’, *Journal of Organizational Computing & Electronic Commerce*, vol. 10, no. 2, pp. 85-101.

Spinellis, D., Kokolakis, S & Gritzalis, S., 1999, 'Security requirements, risks and recommendations for small enterprise and home-office environments', *Information Management & Computer Security*, 7, 3, pp.121.

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

Zernand, M 2003, ‘The Risks and Management of Telework’, *EBS Review,* Issue 16, pp.101-104.

Author/s:
Yang, Huiyi; Zheng, Chaofan; Zhu, Lika; Chen, Fei; ZHAO, YUMIN; Valluri, Manjeera

Title:
Security risks in teleworking: a review and analysis

Date:
2013

Citation:
Yang, H., Zheng, C., Zhu, L., Chen, F., Zhao, Y., & Valluri, Manjeera. (2013). Security risks in teleworking: a review and analysis. Melbourne, The University of Melbourne.

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/33343

File Description:
Security risks in teleworking: a review and analysis