Information Security Strategy and Teleworking (In)security

Millicent Ampomah · Yevindra De Silva · Hanqing Li · Piki Pahlisa · Qian Yang · Qian Zhang

Department of Computing and Information Systems

The University of Melbourne

Abstract

Mainstream writing of teleworking tends to focus on both the economic and social benefits with little emphasis on information security issues. Information security threats of telework however are identified by most literature as a concern for organisations. This literature review examines the different influences on issues leading to information insecurity within the teleworking environment. By drawing on literature, a strategic model for managing and controlling information security threats in teleworking environment is proposed. Organisations essentially needs to implement security measures or controls from a strategic point of view to include formal and informal controls.

Keyword: information security, teleworking, security strategy, information confidentiality, information availability, information integrity.

Introduction

The proliferation of telework in recent times within urban environment has raised a number of information security concerns among organisations. Information security is critical to the success of telework. The objective of this paper is to inspire top organisational management to consider the various aspects of an information security strategy when enforcing teleworking. We do this by proposing a comprehensive information security strategy model to effectively manage and control security issues in teleworking. Teleworking is an alternative form of work structure or work style which makes use of Information Communication Technology (ICT) to enable employees work and interact virtually with colleagues, customers and official workplace without physically being present within a period of time (Day and Burbach 2011). It must be observed in this paper that teleworking is not only limited to working from home but from any environment that is conducive enough to support ICT.

Micro-economic pressures, unanticipated shifts in business environments for competitive advantage and rapid changes in ICT (Teo et al 1998) are the major driving forces behind the redesign of organisational work structure to include telework. A US survey conducted in 2011 by Lister and Harnish (2011) demonstrated a growing number of 61% of employees work from home as teleworkers within the period of 2005 and 2009. This trend is expected to increase in the future as technology advances and employees become more ICT oriented. This means that organisations are more likely to embrace and shift their work structure towards teleworking.

A considerable number of researchers have acknowledged the benefits of teleworking to organisations, individual employees and society on the whole (Niles 1997; Day and Burbach 2011; Tung and Turban 1996; Perez et al 2002; Harpaz 2002). A significant contribution of teleworking to both organisations and employees is greater work flexibility. Due to this, work productivity has the potential to increase since employees can perform their tasks from any geographical jurisdiction. Further, teleworking has been identified as a new way of reducing cost associated with work. This is based on the fact that the cost of real estate is reduced since the need for physical office space and stationary are reduced. Another essential benefit of teleworking is its potential ability to retain experienced employees along with their critical knowledge and insights. Teleworking also reduces fuel consumption and traffic congestion, which help maintain the green environment.

Despite these benefits, there are challenges linked to information security with emphasis on information availability, confidentiality and integrity. This more often than not results in further detrimental effects on individuals and organisations, in particular where an employee task involves access to highly classified and sensitive information. Consequently, this creates a worrying situation at all levels of management as the trend of teleworking is increasingly gaining popularity in organisations.

Previous literature has attempted to address information insecurity associated with teleworking by introducing strategies such as network encryption, authentication and access controls, data compartmentalization and encryption as well as layered defense (James 2011; Peacey 2006). Even though literature has endeavoured to apply security strategies to teleworking in an attempt to protect classified information, the report at hand indicates that information security pertaining to teleworking is still a challenge. This paper focused on this gap to propose a theoretical model to guide effective information security implementation in teleworking.

Methodology

This paper was based solely on a comprehensive literature review that covers substantial relevant academic resources on the topic of “teleworking and security” found using Google Scholar and The University of Melbourne Discovery search engines. Some of the articles used by us are sourced from well-reputed journals such as Information Management and Computer Security. Bolderston (2008) procedure for conducting literature review was applied to examine, identify, categorize and organised security issues into relevant themes. This paper was organised as follows: In the first section, a detailed literature review on the topic was explored and emerging themes were categorised. The next section, which is the discussion, presents our proposed model for effective information security in teleworking based on our findings from literatures. The paper also presented some limitations and future work in this section. The final section presents the closing conclusion of the paper.

Literature Review

Information insecurity is vast; it encompasses technology, processes and people. According to Buurmeijer (1984), information insecurity is the accidental or intentional disclosure, modification or destruction of information. Nonetheless, three underlying information insecurity have been acknowledged; information confidentiality, information integrity and information availability breaches. Information confidentiality breach occurs when stored or information in transit is accessed and read by unauthorised parties. On the other hand, information integrity breach is the alteration of the intended meaning of information by unauthorized persons. Information availability breach is explained as the unavailability of information to authorised person which is sometimes caused by denial-of-service attack.

Although information confidentiality, information integrity and information availability breaches are the main insecurity issues. Scholars have examined other issues of information insecurity related to teleworking. According to various literature, these insecurity issues can be categorized into four aspects including people, physical equipment, organisational and environment. Moreover, each aspect consists of specific security issues. However, these security aspects contribute to the above underlying information insecurity depending on the scenario. Table 1 categorized the identified security issues in teleworking with a brief description of each type of security issue supported by evidences from literature.

Table 1. Summary of the identified information insecurity issues

Security Issues	Literature References
1. People	
a. Lack of security awareness	Teleworkers do not realize the importance of information security. (Peltier 2013; Day and Burbach 2011; Godlove 2012; Funnel 2006)
b. Information disclosure to competitors	Teleworkers breach professional ethics and leak sensitive information to competitors. (Crumbley 2001; Day and Burbach 2011; Godlove 2012; Fairweather 2011; Niles 1997; Sturgeon 1996)
c. Personal safety	Teleworkers are vulnerable to personal injury or a life threatening attack as a result of information insecurity (Ahmad, Maynard & Park 2012; Pasick 2013; Von Bergen 2008)
d. Identification compromised	Teleworkers' identification can be compromised which allows third parties to gain access and make unauthorized modification of sensitive information. (Day and Burbach 2011, Philpott 2008, Sturgeon 1996)
2. Physical Equipment	
a. Theft	The threat of theft of remote devices that are being used by teleworkers. (Scarfone et al. 2009)
b. Unsecure network	Connectivity through public networks will endanger the organisation's information. (Peacey 2006; Scarfone et al. 2009)
3. Organisational	
a. Lack of organisational commitment	Poor organisational commitment increases insecurity. (James 2011; Day and Burbach 2011; Harpaz 2002)
b. Inability to monitor	Difficulties in monitoring the activities of the teleworkers' environment and activities increase security breaches on information. (Pearcy 2006; Peltier 2006)
4. Environment	
a. Interruption/Destruction	Environmental factors such as power failure can interrupt/destruct access to information. (Sturgeon 1996)

People

There is a direct correlation between people and information security. People are considered a substantial element in security, because people act as operators in dealing with data or information systems. Security issues related to people can occur due to teleworkers' weaknesses and intention and the assumption that teleworkers are in possession of sensitive information. These issues are discussed below.

Lack of security awareness

According to Peltier (2013), most security breaches are caused by lack of recognition of security weaknesses. Teleworkers often are not aware that they are a potential source of threat to information security. For instance a teleworker may leave his/her access credentials to an organisation's system boldly written on a paper attached to his/her computer without him/her knowing the dangers of that action. To counter this problem, Day and Burbach (2011) and Godlove (2012) suggested that an organisation need to clearly communicate its security policies through training and casual methods of awareness such as posters to enable teleworkers to have a better understanding about security risks and how to mitigate them. In support of this suggestion, Funnel (2006) stressed the importance of practical skills on security so that teleworkers upgrade their knowledge to overcome security breaches.

Information disclosure to competitors

Sturgeon (1996) and Niles (1997), suggested that teleworkers motivated by economic or ethical reasons could easily hand over sensitive information to their organisation's competitors. Once classified information is accessed by a teleworker, an organisation cannot ascertain that the information will remain within the storage premises of the organisation. Thus, the classified information can easily be handed over to competitors. This may cause the organisation to be out of business if vital information necessary for the business existence is handed to opponents. In order to overcome this issue, Day and Burbach (2011) suggested that the security strategies of surveillance and deterrence could be utilized. In addition, Crumbley (2001) recommended the use enforceable service level agreement between employees and organisations as a strategy of deterrence. Furthermore, Fairweather (2011) recommended that monitoring communication of teleworkers can prevent the disclosure of sensitive information. However, monitoring the communication of teleworkers can be expensive and may infringe on their privacy.

Personal Safety

Personal safety is an issue that is mandated by law to be addressed by organisations, including the ones that opt for the teleworking initiative. Teleworkers are vulnerable to personal injury or even a life threatening attack due to lack of protection in teleworking environment. For instance, teleworkers can be attacked physically for the purpose of providing sensitive information to external parties. Pasick (2013) pointed out that the death of a teleworking engineer might be related to his work and information held outside the conventional workplace. According to Von Bergen (2008), under the law such as the U.S Occupational Safety and Health Act, the organisation is responsible for ensuring the safety of home-based workplaces. In that way, a solution to prevent the issue from occurring is by applying a surveillance strategy that aimed to create situational awareness of threats evolution (Ahmad, Maynard & Park 2012).

Identification compromised

In teleworking worksites, the work is remotely conducted with less supervision from the organisation. This means that it is difficult to identify who is behind the keyboard (Philpott 2008). There is a possibility that the person behind the computer is a third party who succeeds to compromise the teleworker's identification data to gain access to sensitive information or even make unauthorised modification of information (Sturgeon 1996). Therefore, Day and Burbach (2011) suggested that the security strategy of prevention should be applied effectively to ensure that the information would not be modified freely in order to maintain information integrity. In support of this prevention strategy, Sturgeon (1996) recommended the application of appropriate administrative procedures such as password complexity and duration.

Physical Equipment

Teleworkers can utilize computing equipment such as Personal Computer (PC), Smart-phone and Personal digital assistant (PDA) which maybe owned by the teleworkers or by the organisation. The usage of those devices in susceptible public area creates significant security issues due to physical security risk towards the devices that are used for telework. These issues include the chance of being stolen, malicious attack via unsecure networks.

Theft

The devices that teleworkers use may contain critical information of their work. Once these devices are stolen, it means a loss of control of the assets and information (Sturgeon 1996). Competitors or illegal parties may utilise such assets and information and thus the loss poses a threat to the organisation. In order to prevent against an attempt to steal the device, teleworkers need to use physical measure such as cable locks to secure their devices (Scarfone et al. 2009). However, the attempt to protect the physical device must be extended to the information the device holds.

Unsecure network

Public networks at homes, hotels and airports are considered insecure network since anyone can connect to these networks (Scarfone et al. 2009). As a result, teleworkers working in public networks put organisation's network in a vulnerable position where threats such as eavesdropping and man in the middle do not only harm the remote devices but also the internal network of an organisation. Scarfone et al. (2009) recommended prevention strategies to control the risk of the unsecured network by using cryptography method during transmission of data and mutual authentication function between the remote devices and organisation systems. This recommendation is analogous to Peacey (2006) suggestion that countermeasures related to unsecured network should use several prevention technical controls such as the usage of VPN, anti-virus and anti-malware on the devices.

Organisational Issues

In view of the fact that teleworking functionality is closely linked to organisations' resources, then it is imperative that existing organisational resources change to support and sustain teleworking in the area of information security. Important inputs by some authors visibly identified and related organisational commitment, and monitoring to secure information during telework.

Lack of organisational commitment

Interestingly, organisational commitment cannot be exempted from information insecurity issues in relation to teleworking. Some scholars are of the view that lack of organisational commitment towards teleworking has resulted in the many security breaches to classified information (James 2011; Harpaz 2002l). Poor technical assistance by organisations' ICT support to teleworkers contributes immensely to the interception of valid data and critical loss of information, which may result in financial deficit. This is because the ICT support staff may give priority for resolving ICT related issues such as virus attacks of employees who are physically visible to the support staff rather than teleworkers. Thus teleworkers may not obtain the same level of security support as workers at the workplace. As a result, information on teleworkers' devices become more susceptible to security threats of all kinds whilst teleworkers wait in the queue for assistance or seek for assistance from elsewhere.

In the event of obtaining assistance from elsewhere other than the organisation, these teleworkers may fall as preys to social engineering whereby important access credentials may be compromised intentionally. Stone-Gross et al (2011) explained social engineering as the art of manipulating and persuading people to carry out events that are likely to breach information availability, confidentiality and integrity. However, Day and Burbach (2011) attributed lack of trust between teleworkers and their respective organisational ICT support staff to social engineering. In light of poor organisational commitment, there is the need to modify existing ICT structures to oversee ICT issues from teleworkers.

Inability to monitor

Concerns on inappropriate activities conducted by teleworkers whilst connected to the organisation's ICT systems have been established. Some authors have confirmed inefficient monitoring, recording and reporting of unauthorized session and activities of teleworkers may lead to the injection of malware to workplace systems (Pearcy 2006; Peltier 2006). Thus it is much difficult to effectively monitor and control the utilization of the network environment of teleworkers as compared to corporate network. This has been attributed to the different operating systems and applications employed by teleworkers as well as different timezones and schedules of teleworkers. Furthermore, teleworkers often use public network infrastructure to connect to virtual private network, which makes it difficult to detect unauthorized applications and devices that are not controlled by the organisation's ICT support team. Consequently, IP addresses spoofing and other malicious activities can be carried out without notice, creating room for more security attacks that may have ripple effects on the organisation. In this case, the organisation loses substantial amount of money in mitigating the impact of these intrusions on the business.

Environment

The likelihood of security issues in the external and internal working environment of teleworkers' can be caused by interruption and destruction. Sturgeon (1996) argued that the external environment issues are due to lack of safety awareness on the part of the teleworkers. Individual teleworkers' workplace is more likely to be plagued by natural disasters (e.g. fire and earthquake) and crime (e.g. robbery and arson). Internal environment on the other hand is attributed to unreliable power supply, unreasonable structure and lack of emergency equipment (e.g. extinguisher and smoke detectors) at the workplaces of teleworkers (Sturgeon 1996).

Interruption/Destruction

Sturgeon (1996) acknowledged that for teleworkers, the access to information can be lost due to accidental occurrences. A teleworker's workplace, in comparison to official workplaces, is more susceptible to be interrupted by environment factors such as power failure. In this case, teleworkers have to stop their work unexpectedly which may lead to data loss or information transmission disconnection. Additionally, compared with official workplaces, telework locations have low building safety and have a higher vulnerability to catastrophe such as fire and flood (Sturgeon 1996). There is a high risk of information loss, if information created or stored at the telework location is not available outside that location. In order to deal with these security issues, Sturgeon (1996) suggested that organisations should formulate appropriate security awareness program to ensure that their teleworkers can realize the important of security measures and of their ongoing responsibilities. For example, when a teleworkers is selecting his/her home location, he/she should not only consider if the location can satisfy his/her living needs but also security requirements for work. However, it makes sense to have data storage redundancy to prevent loss of information.

Discussion

The findings of this literature review suggested that there were various security issues associated with teleworking initiative. Productivity of the business is interrupted when network of operation of the teleworkers is attacked. Accordingly, these issues have a great impact on financial aspect of an organisation that employs the teleworking initiative. Interestingly, teleworking may prove to be more costly than the anticipated benefits. This is because an organisation may need to additionally invest in sophisticated security mechanisms to safeguard the organisation's reputation and protect sensitive information. Therefore, an organisation needs to consider security aspects including strategies, education, risk assessment, policy and education when implementing the teleworking initiative.

In addition to this, organisations need to consider the relationship between teleworkers and organisation. As stated by Crumbley (2001), the relationships between employees (teleworkers) and employers are not strong as generally accepted and are driven by social and economic pressures. Thus, teleworkers may have poor loyalty to the organisation and motivation to comply with their organisations' security guidelines and policies, which might further deteriorate.

In light of the identified information insecurity issues and the findings of the literature review, an information security model has been proposed in Figure 1. This model illustrated the integration of teleworking business strategies, risk assessment, security strategies, policy, education, measurement

of effectiveness and continuous improvement to change the security mindset of the organisation for effective security implementation. This process is cyclical due to the dynamic nature of business strategy and the risk environment that organisation operates within. Furthermore, this model used continuous measurement of results and improvements based on feedback.

Figure 1: The proposed model for effect information security when teleworking

Business Strategies that influences teleworking needs to be identified by the organisation. This will allow the organisation to identify risks of teleworking that are important to the organisation and needs to be assessed during risk assessment. Our literature review also recognised that different risks require different security strategies. Risk assessment will identify the risks that need to be mitigated and will allow the organisation to determine different security strategies.

Thereafter, the organisation will develop policies to control risks based on the different security strategies. They need to be created in such a manner that it motivates adherence. These policies then need to be communicated to the teleworkers. One of the key aspects of our literature review has been that teleworkers need to understand security issues, the security strategies used to combat them and how the resultant policies are dependent on these security strategies. This will also motivate them to adhere to the policies. This can be done using educational programs that incorporate this change in mindset where teleworkers understand why security is required.

Finally, after implementing the policies, the effectiveness of these policies needs to be measured. This will allow the organisation to know which policies were successful and which did not perform to expectations. Using this as feedback, the organisation will identify what improvements are required. These will be incorporated into the next iteration of the cycle.

The application of this model will result in a changed mindset of security. This change of mindset is where security is now thought of as a continuously improving process where it is understood that each part of the process is not decoupled from other security components.

Limitations and Future Research

This paper contained several limitations; the primary limitation was that the identified security issues are incomplete because they were based only on literature. Majority of the articles do not focus on security in teleworking. Future research should include surveys to ensure the validity of identified security issues by ascertaining the actual financial impact of teleworking initiative in organisations. Moreover, the findings and proposed model (Figure 1) were based on our understanding of the literature and have been influenced by our backgrounds and perspectives. It is necessary to test and refine the findings and the proposed model using empirical evidence.

Conclusion

This paper has explored the potential insecurity pertaining to teleworking. Our discussion emphasises that information security issues can have significant impact on individuals and organisations with further effect on society if not looked at from a strategic viewpoint. There are two major contributions of the study towards information security strategy. Firstly, information insecurities were recognised and categorized according to sources of threat. Ultimately, the proposed model provides a high-level view of information security strategy should be formulated based on the literature review. In particular the model states that business strategy, risk assessment, policy and education should not be viewed as decoupled components of information security and that results should be measured continuously to improve strategy effectiveness. The paper also presented some limitation and areas for future research. In closing, organisations need to realize that existing security strategy for official workplace cannot function effectively in a teleworking environment. This means that organisations may need restructuring their security strategy to support teleworking and in doing so the organisation should consider both technical and non-technical aspects of security strategy.

References

Ahmad, A, Maynard, S, & Park, S 2012, "Information security strategies: towards an organisationalmulti-strategy perspective", *Journal of Intelligent Manufacturing*.vol. 16, pp. 1-14

Anderson, R 2001, "Why information security is hard-an economic perspective", *Computer Security Applications Conference, ACSAC 2001. Proceedings 17th Annual,* pp. 358-365

Bolderston, A 2008. "Writing an Effective Literature Review". *Medical Imaging and Radiation Sciences*, vol.39, pp.86-92.

Buurmeijer, F 1984, "IBM's Data Security Strategy: Some Implementation Aspects", *North-Holland Computers & Security,* vol.3, pp.273-277

Crumbley, DS 2001, "Work structures of the 21st century: implications for the employment law practitioner", *Labor Law Journal*, vol. 52, no. 4, pp.245

Day, FC & Burbach, ME 2011, "Telework Considerations for Public Managers with Strategies for Increasing Utilization", *Communications of the IBIMA*, vol. 2011

Fairweather, NB 1999, "Surveillance in Employment: The Case of Teleworking", *Journal of Business Ethics,* vol. 22 pp. 39-49.

Godlove, T 2012, "Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines", *Information Security Journal: A Global Perspective.*

Harpaz I, 2002, "Advantages and disadvantages of telecommuting for the individual, organisation and society", *Work Study*, vol. 51, no. 2, pp.74 – 80.

James, P 2011, "Are existing security models suitable for teleworking?", *The 9th Australian Information Security Management Conference*

Lister, K & Harnish T 2011, "The State of Telework in the U.S. How individuals, business and government benefit", *Telework Research Network*

Nilles, MJ 1997, "Telework: Enabling Distributed Organizations", *Information Systems Management*, vol. 14, pp. 7-14

Pasick, A 2013, "US engineer's family quits Singapore inquest, insisting he was murdered", Quartz, viewed 10th, July, 2013, <http://finance.yahoo.com/news/us-engineer-family-quits-singapore-044741509.html>

Peacey, A 2006, "Teleworkers – extending security beyond the office", *Network Security Journal*, vol. 2006, no. 11, pp 14-16.

Peltier, TR 2013, "Remote Access Security Issue", *Information Systems Security*, vol.10, no. 6, pp.31-36

Philpott, D 2008, "Teleworking and Coop", *Homeland Defence Journal*

Scarfone K, Hoffman P, & Souppaya, M 2009, "Guide to Enterprise Telework and Remote Access Security, Recommendations of the National Institute of Standards and Technology", *NIST Special Publication,* 800-46 Revision 1.

Schneier, B 2003, "Security Is a Weakest-Link Problem", *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, pp. 103-181

Stone-Gross, B, Abman, R, Kemmerer, R, Kruegel, C, Steigerwald, D, & Vigna G 2011, "The Underground Economy of Fake Antivirus Software", *10th Workshop on Economics of Information Security (WEIS)*

Straub, DW, Goodman, SE, & Baskerville, R 2008, *Information security: policy, processes, and practices*, ME Sharpe.

Sturgeon, A 1996, "Telework: threats, risks and solutions", *Information Management & Computer Security,* vol.4, no.2, pp.27–38.

Sveen, FO, Torres, JM, & Sarriegi, JM 2009, "Blind information security strategy", *International Journal of Critical Infrastructure Protection*, vol. 2, pp. 95-109.

Teo,TSH, Lim, VKG, &Wai, SH 1998, "An Empirical Study of Attitudes Towards Teleworking among Information Technology (IT) Personnel", *International Journal of Information Management*, vol. 18, pp.329-343

Tirenin, W & Faatz, D 1999. "A concept for strategic cyber defense", *Military Communications Conference Proceedings, MILCOM 1999. IEEE*, vol. 1, pp. 458-463

Tung, LL & Turban E 1996, "Information Technology as an Enabler of Telecommuting", *International Journal of Information Management*, vol. 16, pp. 103–117

Von Bergen C.W 2008, "Safety and Workers' Compensation Considerations in Telework", *Regional Business Review,* vol 27

Author/s:
Ampomah, Millicent; DE SILVA, YEVINDRA; Li, Hanqing; Pahlisa, Piki; Yang, Qian; Zhang, Qian

Title:
Information security strategy and teleworking (in)security

Date:
2013

Citation:
Ampomah, M., De Silva, Y., Li, H., Pahlisa, P., Yang, Q., & Zhang, Q. (2013). Information security strategy and teleworking (in)security. Melbourne, The University of Melbourne.

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/33341

File Description:
Information security strategy and teleworking (in)security