Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2011

Are existing security models suitable for teleworking?

Peter James
Edith Cowan University

Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/119

ARE EXISTING SECURITY MODELS SUITABLE FOR TELEWORKING?

Peter James
School of Computer and Security Science
Edith Cowan University, Perth, Western Australia
pjames@securesystems.com.au

Abstract

The availability of high performance broadband services from the home will allow a growing number of organisations to offer teleworking as an employee work practice. Teleworking delivers cost savings, improved productivity and provides a recruitment policy to attract and retain personnel. Information security is one of the management considerations necessary before an effective organisational teleworking policy can be implemented. The teleworking computing environment presents a different set of security threats to those present in an office environment. Teleworking requires a security model to provide security policy enforcement to counter the set of security threats present in the teleworking computing environment.

This paper considers four existing security models and assesses each model's suitability to define security policy enforcement for telework. The approach taken is to identify the information security threats that exist in a teleworking environment and to categorise the threats based upon their impact upon confidentiality of data, system and data integrity, and availability of service in the teleworking environment. It is found that risks exist to the confidentiality, integrity and availability of information in a teleworking environment and therefore a security model is required that provides appropriate policy enforcement. A set of security policy enforcement mechanisms to counter the identified information security threats is proposed. Using an abstraction of the identified threats and the security policy enforcement mechanisms, a set of attributes for a security model for teleworking is proposed. Each of the four existing security models is assessed against this set of attributes to determine its suitability to specify policy enforcement for telework. Although the four existing models were selected based upon their perceived suitability it is found that none provide the required policy enforcement for telework.

Keywords
Teleworking, secure teleworking, security model, security policy enforcement, information security.

INTRODUCTION

There are a number of variations to the definition of what constitutes teleworking (Lister & Harnish, 2011; Access Economics, 2010a). In this paper teleworking is defined as the work practice involving remote computing conducted predominately from homes and occasionally from organised telecentres. Teleworking has a number of distinct advantages for both employee and employer. The employee benefits from reduced travelling time and travel costs, and possibly the opportunity to have flexibility for when the work is to be performed. The employer benefits from reduced office space and attracting talented personnel that would not otherwise be possible due to these individuals not being available to commute and/or work standard business hours. Teleworking can also deliver national economy benefits and improved productivity through reduced traffic congestion, reduced infrastructure maintenance and reduced carbon dioxide emissions (Access Economics, 2010b).

Australia presently lags internationally in levels of teleworking (DBCDE, 2011). With the increase in Internet bandwidth, teleworking has grown more rapidly in countries like the UK and USA (Lister & Harnish, 2011) where it is not uncommon for organisations to offer a telework option to staff. The UK in particular has a long history of teleworking. In the 1980s companies like Xansa (now part of Steria) and ICL (now part of Fujitsu) both established teleworking divisions to enable staff to perform software development from home. A good example of an international company utilising teleworking was Sun Microsystems (now part of Oracle). From the late 1990s Sun Microsystems identified the opportunity to accrue the benefits of teleworking for both the company and its employees and restructured its workforce through the 'Open Work' program (Computer World, 2008). At one stage over 20,000 employees were teleworking part-time or full-time. There are some notable examples of Australian organisations that have more recently implemented teleworking; these include iiNet (Australia's second largest Internet service provider) who has over 150 call centre staff working from home

(Contact News, 2010), and the Queensland Government (Telecommuting, 2009) that allows public servants in some agencies to telework.

The recently published National Digital Economy Strategy (DBCDE, 2011), prepared by the Australian Government Department of Broadband, Communications and the Digital Economy, defines eight digital goals. One of these digital goals aims to increase the teleworking participation rate from 6% of the working population to 12% by 2020. Despite growth of teleworking in many countries there appears to be little research that specifically considers the information security threats and vulnerabilities present in a telework computing environment. The Government lead emphasis on telework in Australia necessitates research is conducted into achieving secure teleworking. The research presented in this paper forms part of an investigation into the methodology, tools and techniques required to achieve secure teleworking.

It is proposed in this paper that a teleworking security model is required and the attributes for such a security model are identified. This paper commences by outlining the rationale for a security model and identifying four existing models that could possibly support secure teleworking. The threats that can arise in a teleworking computing environment are described and categorised according to each threat's impact upon confidentiality, integrity and availability. Possible security policy enforcement mechanisms to counter the proposed threats are enumerated. Using the threats and security policy enforcement mechanisms, the attributes of a teleworking security model are defined. The paper concludes by reviewing the applicability of each of the four identified security models as being a suitable model for secure teleworking.

SECURITY MODELS

A security model provides a security design and analysis tool as it defines the basis for security policy enforcement in a system. A security model is a philosophy that directs the way an organisation approaches security (Liska, 2003). Numerous security models have been defined, with each model addressing one or more of the security policy requirements for confidentiality, integrity and availability of information. Some models are primarily focussed upon defining security policy that is appropriate in defence and government environments whilst others have a more business focussed approach to policy enforcement. Teleworking is a work practice that can be utilised by any organisation; defence, government, commercial or not-for-profit. However, as teleworking is unlikely to be used as a work practice involving the processing of classified defence and government information the existing security models considered in this paper are business oriented rather than defence/government oriented.

Four existing security models have been identified as being possibly suitable for policy enforcement in a teleworking environment. The four security models considered have been described (by their respective authors) at different levels of abstraction which has hindered meaningful comparative analysis, however the required attributes have been identified to enable each models suitability for teleworking to be assessed. Table 1 tabularises the security objectives of each model with respect to confidentiality, integrity and availability of information. A high level overview of each model follows together with rationale on why the security model is considered to potentially provide a policy enforcement philosophy for telework.

Security Model	Confidentiality	Integrity	Availability
Chinese Wall Model	X	X	
Clark-Wilson Model		X	X
Eggshell Model	X		X
Onion Model	X		X

Table 1: Objective of Security Model

Using the SANS definitions (SANS, 2011), confidentiality, integrity and availability are defined as:

- Confidentiality is the need to ensure that information is disclosed only to those who are authorised to view it.
- Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.
- Availability is the need to ensure that the information system is accessible to those who need to use it.

The *Chinese Wall* Model (Brewer and Nash, 1989) deals with both confidentiality and integrity. The objective of the model is to ensure the information of two different users is kept separate, regardless of the relationship and sensitivity/classification of the data, i.e. the model enables access to information to be prevented where a conflict of interest exists. The Chinese Wall model may be a possible enforcement model for teleworking due to its approach to user and data separation.

The *Clark-Wilson* Model (Clark and Wilson, 1987) focuses primarily on preserving the integrity of information, although a secondary attribute of the model is to support availability. The model was defined specifically for business applications. Data integrity is achieved by denying unauthorised modification. The model implements the concept of separation of duties (role based) to enforce information integrity, i.e. information access is controlled by a user's privilege(s) to execute application software that processes the information. The Clark-Wilson model is considered as a possible teleworking security model because of its role based business focus.

The *Eggshell* Model (Bragg et al, 2004) is focussed upon protecting information from unauthorised network access. The security policy for confidentiality is enforced in the model through a perimeter, i.e. access to information is controlled by rules that either allow or prevent entry through the perimeter. As teleworking is a network based activity the Eggshell model may provide a suitable security model.

The *Onion* Model (Bragg et al, 2004) defines layers of control to preserve the confidentiality of information. The model implements the concept of security in depth. Need to know controls are enforced at each layer to control access to information. The layers of security enforced by the Onion model may be appropriate to enforce security for a network based activity like telework.

INFORMATION SECURITY THREATS IN THE TELEWORKING COMPUTING ENVIRONMENT

The lack of physical security in remote locations (compared to a corporate office) and the data processing actions of PC operating systems and applications can result in information security threats that are different to those present in an office based computing environment. The logical and physical security of teleworking PCs will vary between teleworking locations and are unlikely to meet the stringent security commonly in place at office locations. Weaker logical security may make the PC vulnerable to unauthorised access, network and malicious software attacks. Weaker physical security may make the PC vulnerable to unauthorised access, tampering, theft or damage.

The two main information security threats in a teleworking environment (Deloitte, 2011) are considered to be:

- ***Breach of Data Confidentiality on the Internet:*** Data travelling over the Internet may pass through a number of network nodes (e.g. nodes managed by an Internet service provider) before the data reaches its destination. Such nodes provide points of unauthorised access to data. If the data is not protected (e.g. through encryption) it is possible a breach of confidentiality could occur.
- ***Breach of Data Confidentiality in Teleworking Environment:*** The weaker physical and logical security controls, compared to a corporate environment, may result in authorised access to data.

Organisations that recognise these two threats to data confidentiality tend to establish a telework computing environment based upon the secure thin client concept. In a secure thin client configuration data processing occurs predominately on a corporate server, with the teleworker's PC providing a terminal interface to the server and all communication conducted securely over an encrypted virtual private network (VPN) connection. The following scenario provides an example of a secure thin client configuration:

> *A teleworker will initiate a VPN connection over the Internet to a corporate server when commencing work. The teleworker may then use a virtual machine client or a remote desktop client to enable processing to be performed using a set of software applications installed on the corporate server. Very little data processed on the corporate server will be intentionally stored on the teleworker's PC, thus reducing the risk of data loss.*

However, in the above scenario the teleworker's PC operating system and the virtual machine client or the remote desktop client will store and retain temporary copies of data on the local PC, often unbeknown to the user, potentially resulting in the unintended storage of corporate data on the PC. Therefore this thin client approach to telework presents unforeseen information security threats that must be considered.

Alternatively, an organisation may allow a teleworker to process data locally but store information securely on a corporate server. The following scenario provides an example of local data processing:

A teleworker will use a set of software applications installed on the PC and process data locally but ensure the data remains stored on a corporate server. A VPN connection to the corporate server is used to access/transfer data as required. The teleworker is expected to follow company policy and ensure all data is stored on the corporate server and no sensitive data is stored on the teleworker's PC.

In this (local processing of data) scenario, even if the teleworker is diligent in ensuring data is not stored on the PC, the local processing of data will result in the operating system and software applications creating temporary copies.

As a result of the above two scenarios the following information security threats need to be considered:

- ***Sensitive Data Remnants Remaining on a PC:*** The PC operating system and software applications will store temporary data in the form of virtual memory and temporary files on the PC's hard disk drive. Much of this temporary data will remain on the drive after the teleworker has finished work and powered-off the PC. Such data can be readily retrieved through the use of freely available data retrieval/computer forensic tools; a concern if the PC is stolen or if it is disposed of with the hard disk drive still resident in the PC.
- ***Introduction of Malicious Software:*** As teleworking PCs reside outside an organisation a PC may be used by any number of people other than the teleworker (e.g. members of the teleworker's family) who could perform a range of activities that may compromise the PC. Such activities may lead to the PC becoming infected with malicious software which could exploit sensitive data processing and network transactions performed by the teleworker.
- ***Use of Unsecured Portable Storage Media:*** Teleworkers are likely to periodically commute to their employer's offices where they may also wish to transfer sensitive information onto or from portable storage media whilst having access to the organisation's secure network. Portable storage media may be lost or stolen in transit resulting in a possible breach of data confidentiality. Additionally, the portable storage media may become infected with malicious software when used outside the corporate environment. The malicious software could then be transferred to the secure network when the portable storage device is plugged into a networked PC in a corporate office.
- ***System Integrity:*** The integrity of the PC operating system and applications used for teleworking may be affected by accidental or inappropriate actions of the teleworker causing a denial of service and preventing work being performed.

With no specialist IT support on-hand to remediate the impact of the aforementioned threats the consequences can result in lost productivity through teleworkers not being able to work. This set of threats necessitates the identification of a teleworking security model that can be used as the basis for the design of secure teleworking systems.

CATEGORISATION OF THREATS

Traditionally a security model has been defined in terms of its ability to enforce security policy with respect to confidentiality, integrity and availability. To enable the suitability of the four identified security models to be assessed and the most appropriate security model to be identified (from the four or otherwise), the set of teleworking threats enumerated above are categorised (in Table 2) based upon their impact to the confidentiality, integrity and availability to information.

Threat	Confidentiality	Integrity	Availability
Breach of Data Confidentiality on the Internet	X		
Breach of Data Confidentiality in Teleworking Environment	X		
Sensitive Data Remnants Remaining on a PC	X		
Introduction of Malicious Software (Malware)	X	X	X
Use of Unsecured Portable Storage Media	X	X	X
System Integrity		X	X

Table 2: Threat Categorisation

The threat categorisation (in Table 2) shows that the set of threats in the teleworking environment can impact upon the confidentiality, integrity and availability of information. A security model is required that is capable of supporting a range of security policy enforcement mechanisms that will preserve both the confidentiality and integrity of information, and maintain availability to information.

POLICY ENFORCEMENT MECHANISMS

To support the identification and definition of the attributes of an appropriate teleworking security model the potential security mechanisms that could be used for policy enforcement are presented in Table 3.

Threat	Policy Enforcement Mechanisms
Breach of Data Confidentiality on the Internet	Network encryption.
Breach of Data Confidentiality in Teleworking Environment	Authentication, access controls, data encryption.
Sensitive of Data Remnants Remaining on a PC	Data encryption, separation and protection of temporary data, access controls.
Introduction of Malicious Software (Malware)	Separation and protection of computing environment, access controls.
Use of Unsecured Portable Storage Media	Authentication, access controls, data encryption.
System Integrity	Separation and protection of computing environment, access controls.

Table 3: Possible Policy Enforcement Mechanisms

Existing security models are often presented using a formal or semi-formal notation for policy enforcing mechanisms. Usually the notation uses the subject/object concept introduced in the definition of the Bell-LaPadula Model (Bell & LaPadula, 1976). Using the concept of subject (e.g. teleworker, software application) and object (i.e. data file, information source) a definition for each of the policy enforcement mechanisms is given in Table 4 below.

Policy Enforcement Mechanism	Definition
Network encryption	Asymmetric cryptographic technique based upon each subject having a public/private key pair. An object to be transmitted is encrypted with the private key and the receiving subject decrypts using the sending subject's public key.
Authentication	Confirming the correctness of something the subject posses and/or something the subject knows and/or a unique attribute of the subject.
Access Control	Pre-defined permissions assigned to the subject that specify access rights to an object.
Data Encryption	Symmetric cryptographic technique based upon the application of the subject's encryption key to an object.
Separation and protection	Objects are protected within a partition where a subject can only access the partition if it has the correct access rights.

Table 4: Definition of Policy Enforcement Mechanisms

The subject and object definitions for policy enforcing mechanisms presented in Table 4 will enable comparative analysis of the selected four security models to be performed against the required attributes and policy enforcing mechanisms necessary for a teleworking model.

ATTRIBUTES OF A SECURE TELEWORKING MODEL

It is proposed that a teleworking security model is required to provide policy enforcement for the confidentiality, integrity and availability of information, as conceptually modelled in Figure 1. In this proposed security model, confidentiality will be the primary policy objective, with integrity and availability being the respective secondary and tertiary objectives. All of the identified security policy enforcement mechanisms are required to preserve the confidentiality. Subsets of the mechanisms are required to preserve integrity and maintain availability.

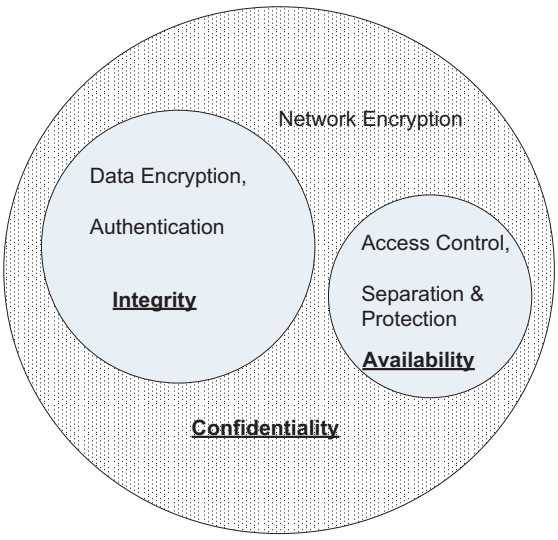

Figure 1: Conceptual Model of Teleworking Security Policy Enforcement

The identified threats and possible policy enforcement measures enable attributes for a teleworking security model to be defined. In summary a security model with the following attributes is required:

- Protect data transmitted over a network.
- Ensure only authorised access to the teleworker's computing environment is achieved.
- Protect the confidentiality of data processed by the teleworker.
- Prevent temporary data and data remnants (created through data processing) being accessed by an unauthorised user.
- Protect the integrity of the teleworker's computing environment and stored data from malicious software and/or user induced damage.
- Protect the confidentiality and integrity of any software and data stored on a portable storage device.
- Ensure the availability of the teleworker's computing environment.

APPLICATION OF AN EXISTING SECURITY MODEL TO TELEWORKING

In this paper it has been hypothesised that a security model appropriate for teleworking is required to enforce policy for confidentiality, integrity and availability. Each of the four existing business oriented security models selected as possibly teleworking security models are considered using the defined teleworking security model attributes and policy enforcement mechanisms presented in this paper.

The Chinese-Wall Model		
Model Synopsis: The model supports policy enforcement for confidentiality and integrity to ensure users and data are separated and protected to ensure no conflict of interest occurs.		
Attribute of a Secure Teleworking Security Model	**Possible Policy Enforcement Mechanism**	**Comments on suitability of the model for teleworking**
Protect data transmitted over a network.	Network encryption.	Model does not consider network security.
Ensure only authorised access to the	Authentication, access controls,	The Chinese Wall model is data

teleworker's computing environment is achieved.	separation & protection.	(object) centric, however it can be implied that a computing environment is protected.
Protect the confidentiality of data processed by the teleworker.	Authentication, access controls, data encryption.	The model supports this attribute.
Prevent temporary data and data remnants (created through data processing) being accessed by an unauthorised user.	Authentication, access controls, separation & protection.	The model supports the intent of the attribute and would enforce policy through the appropriate mechanisms.
Attribute of a Secure Teleworking Security Model	**Possible Policy Enforcement Mechanism**	**Comments on suitability of the model for teleworking**
Protect the integrity of the teleworker's computing environment and stored data from malicious software and/or user induced damage.	Access controls, separation & protection.	Whilst not a stated attribute of the model's policy enforcement definition the model specifies controls that should support the attribute.
Protect the confidentiality and integrity of any software and data stored on a portable storage device.	Authentication, access controls, data encryption, separation & protection.	The model considers data protection at a system level rather than at the portable device level, however its policy enforcement definition should support the attribute.
Ensure the availability of the teleworker's computing environment.	Access controls, separation & protection.	Availability is not a policy objective of the model.
Conclusion: The Chinese Wall model appears to support a number of the attributes of a teleworking security model. However, its key objective is to protect data where a conflict of interest exists, therefore designing a teleworking system using this model is unlikely to produce an appropriate implementation.		

Table 5: Suitability of Chinese Wall Model as a Security Model for Teleworking

The Clark-Wilson Model		
Model Synopsis: This model supports policy enforcement for the integrity of data through a role based approach.		
Attribute of a Secure Teleworking Security Model	**Possible Policy Enforcement Mechanism**	**Comments on suitability of the model for teleworking**
Protect data transmitted over a network.	Network encryption.	The model does not consider network security.
Ensure only authorised access to the teleworker's computing environment is achieved.	Authentication, access controls, separation & protection.	The model supports this attribute.
Protect the confidentiality of data processed by the teleworker.	Authentication, access controls, data encryption.	The model does not support confidentiality.
Prevent temporary data and data remnants (created through data processing) being accessed by an unauthorised user.	Authentication, access controls, separation & protection.	The model's integrity controls provide support for this attribute.
Protect the integrity of the teleworker's computing environment and stored data from malicious software and/or user induced damage.	Access controls, separation & protection.	The integrity controls of the model support this attribute.
Protect the confidentiality and integrity of any software and data stored on a portable storage device.	Authentication, access controls, data encryption, separation & protection.	The model does not support confidentiality, but does support the integrity aspects of the attribute.
Ensure the availability of the teleworker's computing environment.	Access controls, separation & protection.	The model's integrity controls provide support for this attribute.
Conclusion: The Clark-Wilson model supports many of the attributes required for a teleworking security model, however it does not support the enforcement of confidentiality. As protecting the confidentiality of information is important in the teleworking environment the Clark-Wilson model is not considered to be a suitable model.		

Table 6: Suitability of Clark-Wilson Model as a Security Model for Teleworking

The Eggshell Model		
Model Synopsis: The model enforces confidentiality through a perimeter to control access to data. The model is designed for network boundary protection.		
Attribute of a Secure Teleworking Security Model	**Possible Policy Enforcement Mechanism**	**Comments on suitability of the model for teleworking**
Protect data transmitted over a network.	Network encryption.	Although the model is network focussed it does not consider the confidentiality of data 'on the move'. It specifies policy to control access to network nodes.
Ensure only authorised access to the teleworker's computing environment is achieved.	Authentication, access controls, separation & protection.	The model provides boundary protection but if access is permitted no further protection is afforded.
Protect the confidentiality of data processed by the teleworker.	Authentication, access controls, data encryption.	The model provides boundary protection but if access is permitted no further protection is afforded.
Prevent temporary data and data remnants (created through data processing) being accessed by an unauthorised user.	Authentication, access controls, separation & protection.	The model provides boundary protection but if access is permitted no further protection is afforded.
Protect the integrity of the teleworker's computing environment and stored data from malicious software and/or user induced damage.	Access controls, separation & protection.	The model provides some boundary protection against malicious software but provides no protection against user induced damage.
Protect the confidentiality and integrity of any software and data stored on a portable storage device.	Authentication, access controls, data encryption, separation & protection.	The model does not support this attribute.
Ensure the availability of the teleworker's computing environment.	Access controls, separation & protection.	The model's boundary protection provides only limited support for this attribute.
Conclusion: The Eggshell model is a relatively simple model that specifies policy protection for a system against external unauthorised access. Such protection supports some, but not all of the teleworking confidentiality and availability attributes, but does not support the integrity attributes. This model is not considered appropriate for teleworking.		

Table 6: Suitability of Eggshell Model as a Security Model for Teleworking

The Onion Model		
Model Synopsis: The Onion model enforces confidentiality through multiple layers of security.		
Attribute of a Secure Teleworking Security Model	**Possible Policy Enforcement Mechanism**	**Comments on suitability of the model for teleworking**
Protect data transmitted over a network.	Network encryption.	Although the model is network focussed it does not consider the confidentiality of data 'on the move'.
Ensure only authorised access to the teleworker's computing environment is achieved.	Authentication, access controls, separation & protection.	The model supports this attribute.
Protect the confidentiality of data processed by the teleworker.	Authentication, access controls, data encryption.	The model supports this attribute.
Prevent temporary data and data remnants (created through data processing) being accessed by an unauthorised user.	Authentication, access controls, separation & protection.	The model supports this attribute.
Protect the integrity of the teleworker's computing environment and stored data from malicious software and/or user induced damage.	Access controls, separation & protection.	The model focuses primarily on enforcing confidentiality, although the layers of security may provide some integrity protections.

Attribute of a Secure Teleworking Security Model	Possible Policy Enforcement Mechanism	Comments on suitability of the model for teleworking
Protect the confidentiality and integrity of any software and data stored on a portable storage device.	Authentication, access controls, data encryption, separation & protection.	The model considers data protection at a system level rather than at the portable device level, however its policy enforcement definition should support the attribute.
Ensure the availability of the teleworker's computing environment.	Access controls, separation & protection.	The model provides limited support for this attribute.
Conclusion: This high level comparative analysis has shown that the Onion model may be suitable as a security model for teleworking; it certainly appears to be the 'best fit' of the four models considered. However, the layers of security are likely to interfere with the effectiveness of telework. Teleworking does necessitate a 'defence in depth' approach to security.		

Table 7: Suitability of Onion Model as a Security Model for Teleworking

CONCLUSION

This paper has identified and categorised the set of information security threats that exist in a teleworking computing environment and proposed possible policy enforcement mechanisms to counter the threats. Using the categorised threats and policy enforcement mechanisms, attributes of a teleworking security model have been proposed. Each of the four selected security models were analysed using the attributes and policy enforcement mechanisms.

None of the four models were deemed suitable, although all four models displayed some of the attributes required for secure teleworking. The Onion model, in particular, has many of the attributes required of a teleworking security model. However, the multiple levels of security in the Onion model are likely to result in an unwieldy implementation of a security teleworking system.

A security model provides direction for the implementation of a secure information system. The author believes a specific security model for teleworking is required. The research presented in this paper provides the basis for the definition of a teleworking security model. Such a model should be presented in a formal or semi-formal notation to enable the correctness, consistency and completeness of the model to be determined. The author intends to continue the research to define a security model for teleworking.

REFERENCES

Access Economics (2010a). Impacts of Teleworking under the NBN, prepared for the Department of Broadband, Communications and the Digital Economy, Access Economics, July 2010.

Access Economics (2010b) Australian Business Expectations for the National Broadband Network, prepared for the Department of Broadband, Communications and the Digital Economy, Access Economics, November 2010.

Bell, D.E, and LaPadula, L.J. (1976), Secure Computer Systems: Unified Exposition and Multics Interpretation, ESD-TR-75-306, MTR 2997 Rev. 1, The MITRE Corporation, March 1976.

Bragg R., Phodes-Ousley M., et al (2004), Network Security: The Complete Reference, McGraw-Hill/Osborne, 2004.

Brewer D., Nash M. (1989), The Chinese Wall Security Policy, pp.206, 1989 IEEE Symposium on Security and Privacy, 1989.

Clark D. D., Wilson D. R. (1987), A Comparison of Commercial and Military Computer Security Policies, Proceedings of the 1987 Symposium on Security and Privacy, IEEE.

ComputerWorld (2008), Sun's 'Open Work' program sheds light on telecommute savings, June 2008, URL: http://www.computerworld.com/s/article/9105218/Sun_s_Open_Work_program_sheds_light_on_telecommute_savings, accessed October 2011.

Contact News (2010) iiNet hails teleworkers' performance, September 2010, URL: http://www.contactcentres.net/CALLCENTRES/LIVE/me.get?site.sectionshow&CALL1121, accessed October 2011.

Deloitte (2011), Next Generation Telework: A Literature Review for the Department of Broadband, Communications and the Digital Economy, a report prepared by Deloitte Access Economics, July 2011.

Liska A. (2003), The Practice of Network Security: Deployment Strategies for Production Environments, Prentice Hall PTR, Pearson Education Inc., 2003.

SANS, (2011), Glossary of Security Terms, URL: http://www.sans.org/security-resources/glossary-of-terms, Accessed October 2011.

Telecommuting, (2009), Telecommuniting Human Resources Policy, Queensland Government, October 2009, URL: www.health.qld.gov.au/qhpolicy/docs/pol/qh-pol-242.pdf, accessed October 2011.

Lister K., Harnish T. (2011), The Shifting Nature of Work in the UK Bottom Line Benefits of Telework, Telework Research Network, February 2011.