Ready, Steady Telework – Information Security essentials for the teleworker

Umair Jilani, Alwan Ahimmat, Anthony Raso, David Thorpe, and Man Tran

Department of Computing & Information Systems

University of Melbourne

Abstract

We operate and live in an environment where data communication is dependent on Internet connectivity which is decentralised in nature and is not possible to regulate. Due to technology advances, organisations have allowed remote access to their data via the Internet which allows employees to perform work activities via teleworking. Employees have embraced this method of working and teleworking has become a norm in a large number of organisations today.

The problem of teleworking arises as employees are accessing company data outside the organization walls; a potential risk to information leakage whether it be deliberate or unintentional. In this paper the risks associated with teleworking is attributed to physical, technical and document management.

To address these risks, Security Education, Training and Awareness (SETA) and information security policies are important. This paper analyses three core information security objectives in context with SETA i.e. Confidentiality, Integrity and Availability.

The SETA campaign has neither a goal nor content without a security policy, likewise a security policy cannot be enforced without awareness by those for which it is intended.

Introduction

Jack Nilles in 1997 invented the terms “teleworking” and “telecommuting” to define the practice of working in a location that is outside of a traditional office space (Nilles, 1998).

Teleworking is a work practice that involves working remotely. Common arrangements of teleworking include work done at home or in the field or any remote location. The person doing the telework is called teleworker. Telework brings a suite of flexible work practices which are now gaining widespread acceptance. (Daniels, et al., 2001)

Shaw, et al., 2009, states that recently, rapid development in the use of the internet has resulted in huge losses in many organizations due to lenient security resulting in information security awareness becoming an important issue to anyone using the Internet. Organisations are now focusing on reducing the losses therefore making information security awareness a top priority. We agree with Shaw, et al., 2009 in saying that the three main barriers to information security awareness are: (1) general security awareness, (2) employees’ computer skills, and (3) organizational budgets.

With the widespread adoption of teleworking, outsourcing and globalization, security can no longer be an afterthought when teleworking is in the picture.

According to (Peacey, 2006), there are over two million dedicated teleworkers in the UK alone; with an additional 82 million users requiring secure access to the corporate network across the United States and Western Europe. There is therefore a need to raise workforce awareness about potential threats and implementing secure practices. ‘The number of employees who work remotely – often at locations utterly void of security, such as Internet cafes, airport lounges, trains and commuter rails – presents an additional challenge for businesses.’ (Voelz, et al., 2011).

Figure 1 demonstrates the growing adoption of teleworking in the U.S from 2000 to 2010.

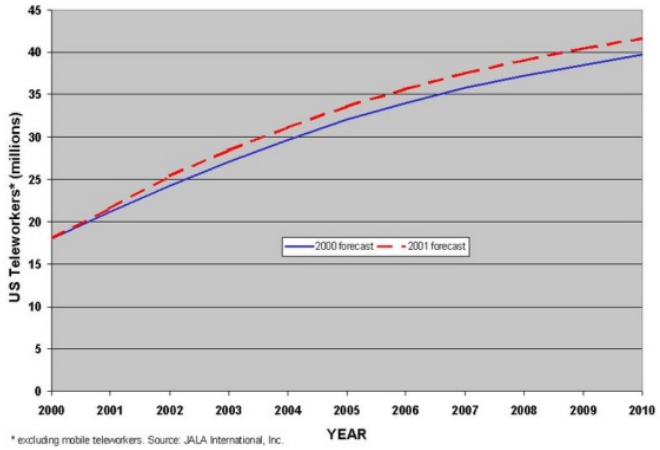

Figure 1. Number of teleworkers in the U.S. (source JALA International)

A goal of the Department of Broadband, Communication and Digital Economy (DBCDE) is to increase the teleworking participation rate in Australia from 6% to 12% by 2020. (James, 2011).

The objective of this paper is to look at the security education, training and awareness (SETA) facets of teleworking. This paper will first provide a literature background that frames SETA issues and key potential risks in the context of teleworkers. Some consequences of information leakage via various facets of teleworking are discussed, along with potential SETA campaign considerations that could be used to counter such risks. It should be noted this paper aims to connect the information security guidelines and teleworkers together not by dictating the content of security policies; but by identifying the risks in the context of their overarching security policies, then identifying various considerations for the development of a supporting SETA campaign.

The physiological and philosophical aspects of SETA including motivation, behaviour and attitude are all important considerations when discussing the development of a SETA campaign; however these are not discussed in detail within this paper. Rather the spotlight is on the facets of awareness required for each of the risk avenues related to teleworking. We acknowledge that culture plays an important role in the risks and development of an effective SETA campaign. We also acknowledge the clear need for security controls on the technology used for teleworking. However this paper will not take culture or security controls into consideration as this is an entire discussion in its own right.

Literature Background

According to (Siponen, 2000) prescriptive security guidelines alone do not create awareness; and may instead see users learning guidelines, yet simply failing to comply with them through lack of effective learning. This results in a clear and present need to develop effective security awareness campaigns, which include content that is relevant and engaging to the target user. In the case of teleworking, it is necessary to develop an awareness campaign that is in context with the effective position of the teleworkers, containing relevant content that is specific to their work environment and conditions. An important consideration is policies and awareness goes hand in hand. The SETA campaign has neither a goal nor content without a security policy, likewise a security policy cannot be enforced without awareness by those for which it is intended.

Teleworkers use various devices including workstations, laptop computers and mobile devices to read and send emails, access websites, review and edit documents, access corporate infrastructure and systems,

and perform many other activities. Many teleworkers use remote access, which is the ability of an organisation's users to access its non-public computing resources from locations other than the organisation's facilities. (Scarfone & Souppaya, 2007). Corporations use an array of technologies to provide remote access such as virtual private networks (VPN) and individual application access (i.e. Web-based mail).

There are numerous research papers which discuss the positive and negative impacts of telework. While some organisational impacts are mentioned in these papers, they are mostly focused on the impacts of teleworking on the end users.

Information Security Risks

The three basic information security objectives are confidentiality, integrity and availability. With teleworking, the dynamics related to these objectives change owing to the fact that teleworkers access corporate information outside of the organisation's security perimeter. For this reason, the need is clear that all employees, partners, contractors etc. need to be educated, made aware and trained on an ongoing basis to constantly support these objectives in their day-to-day teleworking activities.

The primary risks present while teleworking can be broken into three categories:

- Physical Risks
- Technical Risks
- Document Management Risks

Each of these risks includes a number of considerations which are unique to teleworkers, and will be discussed in the following sections.

Physical Risks

Teleworking requires the teleworker to be aware of the physical risks which may impact security.

According to James (2006), the teleworker needs to consider weaker physical security may make the device vulnerable to unauthorised access, tampering, theft or damage. Therefore the teleworker must ensure the device is secured at all times to mitigate such vulnerabilities. In terms of theft, mobile device management (MDM) system exist which allow remote wiping of devices to protect the data however this is only limited to devices such as smartphones and tablets, not workstations, Laptops and portable storage devices.

In additional to theft, portable storage devices can become infected with malicious software when used outside the corporate network. If an infected device is then plugged into a networked device in the secured corporate environment, the malicious software may be introduced to that environment.

Scarfone & Souppaya (2007) suggests implementing physical controls such as cable locks when using devices in hotels or and other locations where third parties could easily gain physical access to the devices.

The teleworker may use public devices such as kiosks or airport lounges to perform their activities. When using such devices temporary data is stored and according to James (2006) this data can be readily retrieved through the use of freely available data retrieval or computer forensic tools.

With the growing adoption of Voice Over Internet Protocol (VoIP) by teleworkers for the purpose of phone conversations, this introduces a new risk requiring consideration.

Teleworkers should be conscious while working in public environment to avoid being a victim of shoulder surfing, that is people looking over your shoulder in order to obtain information. Verbal conversations, be they face to face or over the phone, should also be conducted in a secure manner so as to avoid instances of eves dropping, that is third parties listening in on your conversation.

Technical Risks

According to (Leung, 2007); security threats can be encountered in the forms of users, networks and content. From a technical perspective, we can derive the following potential threats:

User Perspective:

- Device configuration complexity
- Malware
- Password complexity

Network Perspective:

- Denial of service (DoS)
- Eavesdropping (interception)
- Masquerading (impersonation)
- Replay (replaying traffic patterns)
- Network Traffic analysis
- Network Traffic modification

These can be considered a preliminary list of potential technology-centric threats which can exist when teleworking. The threats change frequently and are often specific to the type of organisation and the nature of their business. Furthermore, threats may be of a targeted nature such as corporate espionage, which could lead to some threat avenues being more of a risk than others.

According to (Peacey, 2006), a key concern with many teleworkers is their devices are also frequently used for personal use in addition to work purposes. This is a critical issue when attempting to manage risk, as it not only increases the potential for data leakage; but controls such as security applications (antivirus, anti-malware, firewall) may not function as effectively when compared to those in a corporate environment. These controls may even be compromised as a result of being disabled or uninstalled on "convenience" grounds by the user. Peacey also argues that much of the existing security "layered" architecture is largely irrelevant through it's two dimensional (2D) approach to security as it primarily protects perimeters of the corporate network, yet leaves remote "extensions" exposed such as the teleworker devices themselves.

According to Furnell (2006), users often consider their devices in isolation, devoid of any wider community involvement and by extension, understanding of their impact on other systems or users. A further key point to take is users often perceive their level of security to be higher than it actually is. This clearly identifies a disjoint where users simply do not assume they are a risk because of their false perception of their level of security, which can therefore affect their behaviour and thus lead to security risk exposure.

Document Management Risks

According to Buckland (1998) 'document denotes a textual record'. It is any concrete or symbolic indication, preserved or recorded, for reconstructing or for proving a phenomenon, whether physical or mental.

Document management is the capture, storage and retrieval of documents. These documents contain the details about the organisation, projects, work in progress, contracts, agreements, etc. The documents are assets of an organisation and therefore their security is of high importance.

The activities a teleworker may be engaged in with relation to document management include creation, filing, distribution, retrieval and archiving. To understand why SETA is important when it comes to document management practices of teleworkers, Scarfone, K. & Souppaya has discussed some of the consequences in NIST's report in 2007 about information security. An unauthorised issue of sensitive information which is normally stored in documents could not only damage the public's trust in an

organization but also jeopardize the mission of an organization which may include harming individuals if their personal information has been released. The document management practices include physical and digital copies.

We believe that the information security objective that is most relevant to the document management when teleworking is Confidentiality'. Privacy also plays an important part when it comes to document management risks as 'Privacy is the information that is collected, used and stored by an organization that is intended only for the purposes stated by the data owner at the time it was collected.' (Whitman & Mattord, 2010). This collected data in most of the cases stored in documents of some type. With teleworking becoming more common it is essential to protect these documents by ensuring that the documents are not left unattended at home or any remote location. This includes digital copies of the documents stored on external drives. Details of SETA campaign related to digital copies on portable storage media has been discussed in the Physical Risks section of this document.

Discussion

Within this section, a number of discussion points are made around the identified information security risks. The relation of risks to the development of a SETA campaign is discussed here.

Security policies exist as the foundation for a quality SETA campaign. These policies should be identified clearly and linked within context of the remote teleworker, so as to ensure the user is engaged by the program. If such policies do not already exist within the organisation; there is very little benefit of a SETA awareness program being developed.

From a technical perspective; the primary goal of a SETA campaign is to develop awareness of various security control policies; such as password policies and configuration guides for managing end-user devices. It is also important to provide guidance on what is normal "expected" behaviour of their systems and applications; which should also include clearly defined process and contact details for escalation points for assistance. Furthermore, clear guidance of acceptable use must be provided and enforced, ensuring that users are aware of their obligations and wider ramifications of their resistance to such policies.

An interesting consideration around technical risks, is in methods to develop awareness of their network environment. An example could be developing awareness of the risks of a public (e.g. cafes and airports) vs. private (e.g. home) networks; which carry with them different threats and levels of risk. This area of awareness is however considered largely technical; with many aspects that could be covered through other campaigns, such as developing awareness of expected applications and system behaviour. Furthermore, the content for this category could be somewhat difficult to develop; through the fact that many application and network combinations could be observed, each carrying with them varying levels of risk and complexity. For this area, a SETA campaign in conjunction with security control enforcement (e.g. automated security software status check before allowing VPN connection) would serve to develop both awareness and enforcement of security policies.

The teleworker needs to be constantly aware of the environment in which they are performing their functions as they could be prone to unwanted third parties monitoring.

To address the security awareness issues relating to document management, teleworkers need to understand and realize how confidentiality and privacy can be compromised.

The message that needs to be passed on to the teleworkers in relation to their document management awareness can be classified into three categories. These are creation, storage and distribution. When creating documents, teleworkers need to ensure that there are no local or multiple copies of the documents.

Depending on the physical location different document storage policies apply. Teleworkers need to be aware of these policies and when they apply.

In some organisations documents have classification applied based on the function of the documents. The classifications include unclassified, classified, secret, etc. Ensure that the proper protocols for each of the classification is adhered to with respect to teleworking.

When distributing documents teleworkers need to be aware of and adhere to the document security guidelines. This includes not emailing documents to their personal email addresses. Distribution also includes not printing multiple copies and whenever a copy is printed and taken offsite, teleworkers need to protect it by ensuring it is correctly filed or destroyed if it is not needed.

Sometimes teleworkers need to upload data from a teleworking device e.g. client's data onto the document management system. In this scenario ensure the local copy is destroyed or removed after upload.

Conclusion

Teleworking introduces a high risk of information leakage whether it be deliberate or unintentional.

Teleworking presents a number of information security risks which require appropriate policy supported by an effective ongoing SETA campaign.

When designing a comprehensive and effective SETA campaign it is important to incorporate the physical, technical and document management security risks. Teleworkers not only need to understand but also be educated and made aware of associated risks.

Without a SETA campaign the security policies related to teleworking cannot be prescribed. A security policy acts as a motivator for the SETA campaign and must be developed according to the unique requirements of the organisation.

References

Buckland, M., 1998. Document Numérique. What is a digital document, 2(1), pp. 221-230.

Daniels, K., Lamond, D. & Standen, P., 2001. Teleworking: Frameworks for Organizational Research. Journal of Management Studies, 38(8), pp. 1151-1185.

Furnell, S., 2006. Securing the home worker.. Network Security, 2006(11), pp. 6-12.

James, P., 2011. Are existing security models suitable for Teleworking?. Security Research Institute Conferences, 1(Australian Information Security Management), p. 11.

Leung, A. S. Y. C. H., 2007. The security challenges for mobile ubiquitous services. Information Security Technical Report, 12(3), pp. 162-171.

Nilles, J., 1998. Some Common —and Not So Common— Telework/Telecommuting Questions. 1 ed. Los Angeles: Jala International, Inc..

Peacey, A., 2006. Teleworkers – extending security beyond the office. Network Security, Issue 11, pp. 14-16.

Scarfone, K. & Souppaya, M., 2007. User's Guide to Securing External Devices for Telework and Remote Access, Gaithersburg: NIST.

Shaw, R., Chen, C. C., Harris, A. L. & Huang, H.-J., 2009. The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), pp. 92-100.

Siponen, M. T., 2000. A conceptual foundation for organizational information security awareness.. Information Management & Computer Security, 8(1), pp. 31-41.

Slusky, L. P.-N. P., 2012. Students Information Security Practices and Awareness.. Journal of Information Privacy & Security, 8(4), pp. 3-26.

Voelz, G., Lindsay, M. & Don, P., 2011. Counterintelligence and Operational Security, Florida: Government Training Inc.™.

Whitman, M. E. & Mattord, H., 2010. Management of Information Security. 3rd ed. Boston: Cengage Learning.

Author/s:
Jilani, Umair; Ahimmat, Alwan; Raso, Anthony; Thorpe, David; TRAN, MAN

Title:
Ready, steady telework: information security essentials for the teleworker

Date:
2013

Citation:
Jilani, U., Ahimmat, A., Raso, A., Thorpe, D., & Tran, Man. (2013). Ready, steady telework: information security essentials for the teleworker. Melbourne, The University of Melbourne.

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/33342

File Description:
Ready, steady telework: information security essentials for the teleworker