The Characteristics of Smartwork Security Compare to Traditional Telework

Young-Jin Choi [1] , JongHei Ra [2], DongIk Shin[3] and Yong-Gyu Jung[4*],

[1] Department of Healthcare Management, Eulji University.
212, Yanggi-Dong,Sujung-Gu, Sungnam-Si, Korea
yuzin@eulji.ac.kr

[2]Department of Logistics&Distribution, Gwangju University.
277 Yeoduck-Ro, Nam-Gu, Gwnagju, Korea,
jhra@gwangju.ac.kr

[3] Department of e-Marketing, HongIk University.
2639 Sejong-Ro, Jochiwon-Eup, Chungnam, Korea
dishin@hongik.ac.kr

[4] Department of Medical IT and Marketing, Eulji University.
212, Yanggi-Dong,Sujung-Gu, Sungnam-Si, Korea
ygjung@eulji.ac.kr, Corresponding author

Abstract

Smartwork has been thought to satisfy both employee and company's interests. Nonetheless, there are critical barriers of introducing smartwork because of security problem. In order to derive threats and vulnerabilities of smartwork, we derive threats through structured interview with heavy users or designers of smartwork, then verify the derived threats by survey. Three layers, which are devices/networks/servers, are proposed as a common framework for analyzing characteristics of two types of smartwork.

Keywords: *Smartwork; Telework; Security; Threats; Vulnerability; Home-based, Mobile office*

1. Introduction

Recently, according to the concern of environmental pollution and quality of life, smartwok has been increasing. Smartwork refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities [8]. Smartworkers use various devices, such as desktop and laptop computers, smartphones, and PDAs, to read and send email, access Web sites, and perform many other tasks. In this case, most smartworkers use remote access, which is the ability for a company's users to access its nonpublic computing resources from locations other than the company's facilities.

For many years, home-based smarkwork was the primary method, but increased mobile devices have allowing for expanded to mobile office. Mobile office is the ability for an organization's employees to perform work from external locations using mobile devices.

Smartwork has been thought to satisfy both employees and a company's interests, which are usually contradictory. Nonetheless, there are critical barriers of introducing smartwork because of security issues. Proper introduction of smartwork requires a security protection model which allows efficient management of threats and vulnerabilities [1, 2, 3, 9]. These can be accomplished through a combination of security features built into the remote access solutions and additional security controls applied to the smartwork devices [6].

Even though, previous literature show diverse type of security model, but those are not applicable to smartwork because previous models often focus on home-based or mobile security at the individual level, not include the security of business process and information.

This study attempts to develop security management framework including overall smartwork characteristics. In order to derive threats and vulnerabilites of smartwork, we conduct literature review. Also, we derive threats through structured interview with heavy users or designers, and verify the derived threats by survey. The framework, which is consist of devices/networks/servers, is proposed as a common framework for analyzing characteristics of smartwork comparing to traditional telework.

2. Related Works

After introduced by Nilles [5] as ‘telecommuting’, smartwork can be thought similar to telework. But, it emphasizes workspace mobility, cooperation between workers, and organizational efficiency. Smartwork can be classified into home-based and mobile office. The home-based smartwork is the oldest type, that built the information and communication facilities to work at home.

And, mobile office used smartphone, PDA and laptop without spatial constraints conducting business in anywhere. Despite the many advantages, smartwork are exposed to various threats. In particular, security threats at mobile devices increase the corporate information disclosures.

Most of studies on smartwork security are based on the concept of telework. For example, NIST [6] suggested as major threats to remote access as follows: lack of physical security controls, unsecured networks, infected devices on internal networks, external access to internal resources. Turpin [10] classified security into four groups, those are compose of physical access to the users pc, access through the Internet, access through the network, and viruses. Paul [3] identified major threats as follows: mobile apps, social network-based scams, fake antivirus, PDFs, war games. Microsoft [4] argued the importance of linking organizational objectives with telework services. And, showed potential threats, those are spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

Specially, the threats for mobile devices stem mainly from size and portability, and wireless interfaces. Size and portability can result in the loss of physical control of a device. Also, wireless interfaces such as cellular and Bluetooth provide additional threats. They can also be used to deliver malware, the same as with non-subscription wireless interfaces such as Bluetooth. In sum, security threats to mobile handheld devices include loss or disposal, unauthorized access, malware, spam, electronic eavesdropping, electronic tracking, cloning, server-resident data [8].

Most of previous studies on smartwork threats focus on physical security and logical security, and classify smartwork layers into terminal, server/platform, and network.

3. Research Methodology

Smartwork security still is not arranged, and rapidly changed to mobile environment, the related technologies are evolving and added. In this case, qualitative and quantitative methods can work iteratively to derive a more complete understanding of the phenomenon under study. The study was conducted in accordance with the following procedure:

The first stage was qualitative, which used to identify relevant dimensions of smartwork security risk. In this stage, articles and books were reviewed if the terms “Smartwork security risk”, or ‘‘Telework security risk’’, or ‘‘Telework security vulnerability’’ were in the title or key words. Through this course, we extracted 20 relative items. And the second, to arrange the items executed the following procedure: item reduction, initial grouping, regrouping, and synthesizing.

Step1 Item reduction: All items with the same or very similar meaning were regarded as the same; thus redundancy was eliminated.

Step2 Initial grouping: Each individual was asked to group the items by looking for similarities.

Step3 Regrouping: Each individual was asked to regroup the items by looking for subtle similarities and differences between groups. It could lead to new categories and concepts that the investigators had not anticipated.

Step4 Synthesizing: All five individuals worked together in trying to achieve consistency in the groupings.

As a result, 13 items were identified, representing three different dimensions. The third, selected items were included in the survey instrument. Each was worded as a statement and measured on a five-point Likert scale ranging from ‘‘not important at all’’ to ‘‘most important’’. In order to determine the level of smartwork’s vulnerability, the survey was executed to 62 users and operators.

4. Results

Through the research procedure, we classified the smartwork security layer to devices, networks, and server. And 13 items arranged to 3 layers like as table1. Risks of different types are as follows. The score range of home-based is from 1.1 to 3.5, and standard deviation is 0.62. The score range of mobile office is from 1.5 to 3.3, and standard deviation is 0.58. The average scores are home-based(2.4), mobile office(2.4), there is no significant different.

Table 1. The Score of Layer and Type

Layers	Types	
	Home-based	Mobile Office
Devices	2.5	2.9
Networks	2.5	2.2
Servers	2.4	2.1

Comparing risks among three layers gives the following results: device(2.7), network(2.3), server(2.3). Device layers are higher than network and server. The results are stem from pervasive mobile devices, those are not managed importantly in the past.

Considering layers and types together, several significant characteristics can be derived. At the device layer, the mobile office threat is higher than home-based. The result may reflect recent circumstances, that are many people and companies are used mobile devices and the mobile devices have lots vulnerabilities like as loss and theft.

At the network layer, home-based score is higher than mobile office. Specially, there are difference at arbitrary network and electronic eavesdropping. At server layer, home-based score is higher than mobile office. Specially, there are difference at Exposure data through server weakness and Unauthorized parties access to remote server.

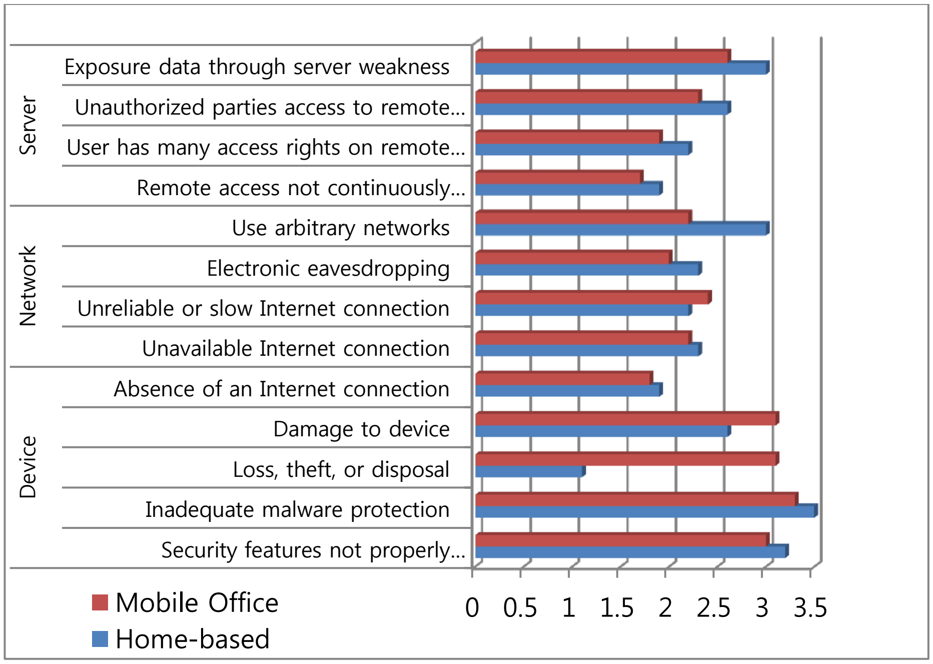

Figure 1. The Characteristics of Smartwork Threats

5. Conclusion

To find the characteristics of smartwork security threats and managed framework, we reviewed the former researches and selected the items. And, the items categorized three layers, that are consist of device, network, and server. Also, conducted survey with smartworker, and summarized the results in table1. Following the survey results, there is no significant difference between home-based and mobile office, but layers have some difference. Specially, device layers have to be controlled carefully in the smartwork condition. The study includes “personal devices” as a major threat item, and evidence shown in the study also supports this notion. Even though those contribution, there are some limitation and future research items. A control model mitigating threats identified in the study must be carried out in near future.

References

[1] Coso, Enterprise Risk Management-Integrated Framework, Executive Summary, **(2004)**.

[2] DOD(Department Of Defense) 8510.1-10, Department of Defense Information Technology Security Certification and Accreditation Process(DITSCAP), **(2007)** November.

[3] Ian Paul, "Five Big Security Threats for 2011", PCwolrd, **(2011)**, http://www.pcworld .com/article/221780/five_big_security_ threats_for_2011.html.

[4] Microsoft, “TELEWORK PLANNING CONSIDERATIONS : A RISK-BASED APPROACH FOR IT MANAGERS”, A Microsoft U.S. government white paper , **(2011)**.

[5] J. M. Nilles, F. R. Carlson, P. Gray and G. J. Hanneman, “The Telecommunications- Transportation Tradeoff”, Wiley, **(1976)**.

[6] NIST, SP 800-56, Guide to Enterprise Telework and Remote Access Security, **(2009)** June.

[7] NIST, SP 800-114,User’s Guide to Securing External Devices for Telework and Remote Access, **(2007)**.

[8] NIST, SP 800-124, Guidelines on Cell Phone and PDA Security, **(2008)**.

[9] T. Godlove, “Telework and Mobile Computing : Security Concerns and Risks”, The security Journal, Vol.30, pp. 5-11, **(2010)**.

[10] P. Turpin, “Securing Telecommuters : Possible threats and Solutions”, Global Information Assurance Certification Paper, **(2004)**.

Authors

Young-Jin Choi

1988 Master of Business Administration, Hankuk University of Foreign Studies

2004 Doctor of Business Administration, Sungkyunkwan University

2006-present professor in the Department of Healthcare Management, Eulji University

<Interest areas: IT Governance, Medical Information Systems>

JongHei Ra

2001 Doctor of Computer Science, Sungkyunkwan University

2001-present professor in the Logistics Management, GwangJu University

<Interest areas: Cloud Computing, Green Data Center, Performance Evaluation >

DongIk Shin

1993 Doctor of Business Administration, University of Nebraska

1999-present professor in the e-Marketing, HongIk University

<Interest areas: Enterprise Architecture, IT evaluation, IT Audit>

Yong Gyu Jung

1981 BS Seoul National University

1994 Master of Engineering, Yonsei University

2003 Doctor of Science, Kyonggi University

1999-present, professor in the Department of IT marketing, Eulji University

<Interest areas: Clinical Data Mining, Medical Information Systems,
EDI Standards (UNEDIFACT, ebXML)>