International Journal of Service and Knowledge Management
International Institute of Applied Informatics
2022, Vol. 6, No. 1, IJSKM642

Risk Assessment for Mobile Workers based on Multiple Viewpoints and Portfolio of Risk Countermeasures

Tenzin Dechen [*], Sonam Wangyal [*], Shigeaki Tanimoto [*], Hiroyuki Sato [†], Atsushi Kanai [‡]

Abstract

In recent years, the government-led "work style reform" has been heavily promoted, and the work style called telework has been attracting attention, particularly since the advent of COVID-19 in early 2020. Telework, which involves mobile workers working outside the office to improve productivity and reduce costs, is becoming mainstream in many companies. However, as workers outside of the office perimeter face increasing daily security threats, mobile workers present various new risks to enterprises. Mobile workers themselves are also associated with risks due to changes in their working environment, as the increasing external pressures to work more effectively and efficiently can affect their well-being. In this paper, we focus on risk, which is the most important of the various issues facing mobile workers. Specifically, we extracted the current risk factors of mobile workers by using a risk breakdown structure method based on literature and case studies, and then proposed countermeasures for the extracted risk factors using a risk matrix method. We also developed a portfolio of risk measures from the viewpoint of practicality and demonstrated that step-by-step measures are possible. Finally, we evaluated the effectiveness of the proposed risk measures using the risk values. Our findings will help contribute to a safe and secure mobile work environment.

Keywords: Mobile workers, Mobile workforce, Risk breakdown structure, Work-life balance

1 Introduction

With the advent of COVID-19 in early 2020, telework has rapidly become more and more popular. Furthermore, the advancement of technology combined with ever faster connectivity has led to enterprises witnessing rapid changes in the workforce. For example, as the critical data of enterprises are increasingly shifted onto the cloud, workers are no longer confined within the office premises and can now access data from all networks and any location. The use of mobile workers is reaping benefits in terms of productivity for businesses and reduced budgets for technological consumption. It can also provide benefits to small businesses in terms of real estate

[*] Chiba Institute of Technology, Chiba, Japan
[†] The University of Tokyo, Tokyo, Japan
[‡] Hosei University, Tokyo, Japan

costs. Moreover, it is beneficial for the workers themselves, as they can continue to work from any desired location, which significantly reduces the cost and environmental effects of travel [1]. Enterprises all over the world are attempting to increase their business competitiveness by allowing workers to work remotely and introducing new workspace environments outside of the office.

According to Strategy Analytics reports, the global mobile workforce is set to increase from its prior total of 1.45 billion in 2016, accounting for 38.8% of the global workforce, to 1.87 billion in 2022, accounting for 42.5% [2]. Mobile working is increasingly becoming the norm for many enterprises. However, despite the apparent benefits, this mobile working trend has significantly increased the risk of data breach. For example, mobile workers' use of personal devices, along with their engagement in risky online behavior and use of free unsecured Wi-Fi networks, carries the risk of exposing their companies' confidential information and can lead to several other vulnerabilities as well. Moreover, as the mobile workers are operating beyond the layered defense security of offices [3], enterprises are facing difficulties in effectively managing the workers, and their confidential data are at a constant risk of being disclosed to unauthorized groups or individuals.

Against this background, we focus in this paper on risk, which is the most important of the various issues facing mobile workers. Specifically, Section 2 describes the current status of mobile workers, including a literature review, case studies, and related research. Section 3 presents the results of a risk assessment for mobile workers based on the survey results in Section 2. Section 4 presents a portfolio of the risk measures proposed in Section 3 from the perspective of practicality. In Section 5, we summarize the paper and discuss future issues. The contributions of this work will help lead to the realization of a safe and secure mobile work environment.

2 Current Status of Mobile Workers

2.1 Overview of Mobile Workers

Mobile workers are defined as individuals who move to and from different locations while utilizing information and communication technology [4]. With mobile workers predicted to account for almost 50% of the global workforce by 2022, this trend potentially represents a huge challenge to enterprises. A recent survey of mobile security reports by iPass states that in a poll of 500 CIOs and senior IT decision makers from the U.S., the U.K., and Germany, more than half (57%) of respondents suspect that one or more of their mobile workers has been the victim of a cyber-attack or has faced mobile security threats [5]. Major security issues mainly stem from irresponsibility on the part of workers. A survey by Apricon states that 18% of the employers believe that their mobile workers do not care about security at all, suggesting that workers often prioritize convenience over security [6]. A 2008 Cisco survey conducted by InsightExpress states that remote workers were more negligent about security and less vigilant in practicing secure online behavior due to their belief that the Internet was becoming more secure [7].

Mobile working has multiple well-known benefits, with flexibility being the most obvious. Flexibility enables workers to fulfill both their work and private life responsibilities and thereby assists in their achieving work-life balance. In a work-life balance survey, researchers found that employees believe flexible working practices improve workplace morale, which might positively influence work-life balance [8]. However, studies have also shown that being constantly connected to the office through a smartphone leads to an erosion of the boundaries between work and non-work.

Moreover, mobile workers face increasing external pressure to work more effectively and efficiently throughout the working day or week. They feel compelled to work longer hours and tend to make themselves constantly available via their tablet or smartphone and are surrounded by their work most of the time [9]. A variety of adverse behaviors such as reducing daytime breaks and routinely checking work email have also been reported, which could affect the well-being of the workers.

2.2 Related Works

In prior research on the risks of mobile workers, the main focus has been the cyber aspects. Non-cyber aspects such as physical and psychological aspects should also be considered in the mobile worker risks. For example, Mulki et al. (2009) have addressed the critical issues related to internal communication, social interaction, and employee satisfaction in an effort to understand remote worker challenges [10]. Boswell et al. (2007) investigated how the use of communication technologies beyond normal work hours relates to work-related attitudes and work-to-life conflict [9].

In our research, we have also considered non-cyber aspects such as the general health of employees, changes in working habits, lone working, and so on through a comprehensive viewpoint using the Risk Breakdown Structure (RBS) method [11].

We have previously described the identification of risk factors for the risk assessment of mobile workers [12], reported the results of a detailed risk assessment based on this identification, and identified specific risk measures [13]. However, the practical evaluation of the proposed risk measures has been insufficient. In this paper, we clarify a new portfolio of risk countermeasures to enable the gradual application of risk countermeasures to mobile workers. This will contribute to the safe and secure operation of mobile workers.

3 Risk Assessment of Mobile Workers

Generally, risk assessment is conducted in the following order: (1) risk specification, (2) risk analysis, and (3) risk evaluation [11].

3.1 Risk Specification of Mobile Workers

3.1.1 Extraction of Risk Factors

In this paper, we systematically extracted 20 different risk factors from a comprehensive viewpoint using the Risk Breakdown Structure (RBS) method, which is a typical method in the risk management field. The risks are listed in Table 1, which classifies the results on the basis of a hierarchical viewpoint of the risk factors of mobile workers [13].

As shown in the table, the risk factors of mobile workers are classified into human factors and social and environmental factors on level 1 of the RBS hierarchy. The human factors in the mobile workforce are perhaps the biggest challenges in terms of cyber security. Human error is the leading cause of data and security breaches. Since workers, i.e., mobile workers, and outsiders, i.e., malicious or unauthorized persons, are the most precarious entity in the mobile workforce, we further classified the human risk factors into risk caused by workers and risk of outsiders to enterprises on level 2. As for social and environmental risks, they are generally acquired by the workers due to changes in their working environment and routine. Examples include inadequate work-life balance, general health, and so on.

Table 1: Risk specification of mobile workers.

	Level 1	Level 2	Risk Factors	Contents
1	1. Human Factor	1.1 Workers	1.1.1 Access of work files with personal, non-IT-protected device	Risk of accidental loss of data, misuse of data
2			1.1.2 Use of work devices for personal use	Mixture of employee's private and work-related data on work device
3			1.1.3 Access of unapproved sites, consumer apps, suspicious emails	Risk of malware attacks, computer virus infection
4			1.1.4 Non-compliance with security practices	Risk of security breach
5			1.1.5 Leaving confidential documents unattended	Risk of mismanagement of confidential documents
6			1.1.6 Leaving devices unattended	Risk of exposing confidential data to unauthorized person
7			1.1.7 Sharing of computer and devices	Risk of unauthorized access and misuse of information by individual
8			1.1.8 Use of unsecured Wi-Fi communications	Leakage of information during connection to public WiFi
9		1.2 Outsiders	1.2.1 Device loss or theft	Loss of confidential data or data in hand of malicious person
10			1.2.2 Shoulder hacking	Procurement of personal and confidential data by shoulder hacking
11			1.2.3 Intruders gaining access to sensitive information	Easy to steal and procure information
12			1.2.4 Eavesdropping attacks	Easy to eavesdrop and obtain data over unsecured network
13	2. Social and Environmental risk	2.1 Inadequate work-life balance		Hard to separate personal life and professional life
14		2.2 Lone working		Risk of stress, feeling isolated, risk to physical and mental health
15		2.3 Invasion of personal space in office-related work		Increases in physiological stress, loss of privacy
16		2.4 General health and safety hazards		Risk of suffering an accident, illness while working alone
17		2.5 Change in working habits		Feeling of restlessness, frustration, and indecisiveness
18		2.6 Inadequate resources		Lack of required resources may lead to inability to work
19		2.7 Lack of face-to-face communication		Social isolation, feeling uninvolved and unproductive
20		2.8 Lack of self-motivation and encouragement from employer		Feeling unmotivated and unproductive

3.1.2 Features of Risk Factors

Out of the 20 extracted risk factors, some risks may have a higher tendency to cause a huge liability and cost for the company. Identifying and prioritizing risk is therefore important in terms of appropriately applying limited resources and maximizing the use of available resources. These risks can be prioritized based on how critical the impact would be and the likelihood of the risk. As shown in Table 2, we have highlighted the major risk factors in each category.

Table 2: Major risk factors.

Classification		Risk Factr
Human Factor	Worker	1.1.2 Use of work devices for personal use
		1.1.4 Non-compliance with security practices
		1.1.8 Use of unsecured Wi-fi Communications
	Outsider	1.2.1 Device loss or theft
		1.2.3 Intruder gainning access to sensitive information
Social and environmental		2.1 Inadequate work-life balance
		2.2 Lone working
		2.5 Change in working habits

(1) Major Risk in Human Factor

Human factors are classified into risk caused by workers and risk of outsiders to enterprises. In the worker's category of the human factor, the major risk concerns workers' non-compliance with security practices. Employees who do not comply with information security policies are a serious risk for their companies. As stated earlier, since the workers are outside of the secured perimeters of the office environment, enterprises are facing difficulties in effectively managing the workers, and their confidential data are at a constant risk of being disclosed to unauthorized groups or individuals.

Use of unsecured Wi-Fi communication is another notable risk factor. Mobile workers frequently work from public places on laptops and personal devices, and when working at any public area, it is convenient to connect to free public Wi-Fi, which is often not secure. This convenience of using an unsecured Wi-Fi network can expose private and corporate information to anyone snooping on that network.

Another major risk is the risk of intrusion. Since the workers are outside of the secured perimeters of the office environment, it is easier for hackers or masqueraders to procure confidential information, and therefore, intrusions are more likely to occur often. To avoid or decrease the risk of intrusion into company systems, continuous network monitoring should be performed.

(2) Major Risk in Social and Environmental Factor

In the social and environmental factor, inadequate work-life balance is a major concern for mobile workers. Work-life balance can be defined as a state of equilibrium between a person's job and personal life. Despite the benefits of flexibility and convenience, mobile workers are subjected to inefficient work-life balance. Research shows that being constantly connected to a smartphone leads to an erosion of the boundaries between work and non-work.

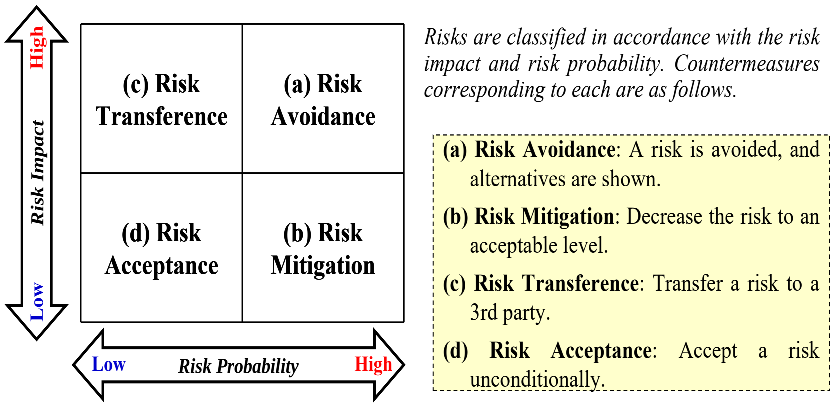
Lone working is another major risk concerning mobile workers, many of whom are associated with lone working. The Health and Safety Executives (HSE) defines a lone worker as "those who work by themselves without close or direct supervision". Lone workers can face hazards similar to those of other workers, but the risk involved may be greater since the workers are on their own.

3.2 Risk Analysis of Mobile Workers

We conducted the risk analysis using the risk matrix method, which is commonly utilized in the risk management field. We then deduced countermeasures on the basis of the results.

This method classifies risks into four types in accordance with their risk probability and risk impact (as shown in Fig. 1): Risk Transference, Risk Mitigation, Risk Acceptance, and Risk Avoidance. It also provides guidelines on how to draw up countermeasures [14], [15].

We took the classifications of the risk matrix methods along with their proposed countermeasures listed in Table 1 and analyzed the 20 risk factors by using the risk matrix method. Table 3 shows the risk countermeasures we proposed for the risk factors of mobile workers in Table 1 using the risk matrix method in Fig. 1.



Risks are classified in accordance with the risk impact and risk probability. Countermeasures corresponding to each are as follows.

(a) Risk Avoidance: A risk is avoided, and alternatives are shown.

(b) Risk Mitigation: Decrease the risk to an acceptable level.

(c) Risk Transference: Transfer a risk to a 3rd party.

(d) Risk Acceptance: Accept a risk unconditionally.

Figure 1: Risk matrix method.

Table 3: Risk analysis results.

No.	Level 2 /Risk Factors	R.I	R.P	Risk Classification	Risk Countermeasure
1	1.1.1 Access of work files with personal devices	H	L	Risk Transference	Setting up a virtual desktop infrastructure (VDI) or mobile device management protocol to separate company data from personal data.
2	1.1.2 Use of work devices for personal use	L	L	Risk Acceptance	Clearly define appropriate policies and related procedures, placing particular emphasis on personal use.
3	1.1.3 Access of unapproved sites, comsumer apps.	L	L	Risk Acceptance	Offer regular training and awareness campaigns to make employees aware of the risks and potential consequences.
4	1.1.4 Non-compliance with security practices	H	L	Risk Transference	Actively involve employees in defining and monitoring the security of company assets.
5	1.1.5 Leaving confidential documents unattended	H	L	Risk Tranference	Educate and train employees on standards, guidelines, and procedures for handling companys' documents.
6	1.1.6 Leaving devices unattended	H	L	Risk Tranference	Utilize computer locks, device management applications, and suites to help secure business data.
7	1.1.7 Sharing of computer and devices	L	H	Risk Mitigation	Encrypt critical data. Enforce strong password, multifactor authentication tools and session security configuration.
8	1.1.8 Use of unsecured Wi-Fi communications	L	H	Risk Mitigation	Avoid using public Wi-Fi, unless appropriate security measures (e.g., VPN connection) are implemented.
9	1.2.1 Device loss or theft	H	H	Risk Avoidance	Install mobile device management (MDM) solution on devices. Implement an insurance policy so companies can protect themselves against financial loss.
10	1.2.2 Shoulder hacking	L	H	Risk Mitigation	Implement shoulder hacking preventive measures decided by the enterprise.
11	1.2.3 Intruders gaining access to sensitive informat	H	L	Risk Tranference	Perform continuous network monitoring using advanced and up-to-date technology.
12	1.2.4 Eavesdropping attacks	H	L	Risk Transference	
13	2.1 Inadequate work-life balance	L	H	Risk Mitigation	Introduce well-balanced policies that take into account both the risks and advantages for both the company and its employees.
14	2.2 Lone working	H	H	Risk Avoidance	Encourage regular communication among workers and provide opportunities to have face-to-face discussions with employers.
15	2.3 Invasion of personal space due to office-relate	H	H	Risk Avoidance	A separate work setting environment or office is highly recommended.
16	2.4 General health and safety hazards	H	L	Risk Transference	Implement regular monitoring and enquiries to make sure employees are following safe practices.
17	2.5 Change in working habits	H	H	Risk Avoidance	Setting up regular forums to discuss employees' work and concerns.
18	2.6 Inadequate resources	L	H	Risk Mitigation	Implement enquiries and updates on work-flow to ensure workers requirements are met.
19	2.7 Lack of face-to-face communication	L	H	Risk Mitigation	Use of social tools to make employees feel involved. Develop channels that connect the workplace community.
20	2.8 Lack of self-motivation and encouragement	L	L	Risk Acceptance	Encourage consultation and involvement. Set up regular forums to discuss employees' work and concerns.

Reference: **R.I** = Risk Impact; **R.P** = Risk Probability; H = High; L = Low

3.3 Risk Evaluation of Mobile Workers

We evaluated the validity of our proposed countermeasures through a quantification of the risk factors shown in Table 3. We utilized a risk formula commonly used in the ISMS field and then calculated the risk value on the basis of our previous qualitative results. Finally, the risk value was deduced by using the formula and approximation [16].

3.3.1 Risk Formula

(1) Ordinary Risk Formula

In general, each risk value is quantified as

$$\textit{Risk value} = \textit{value of asset} \times \textit{value of threat} \times \textit{value of vulnerability} \qquad (1)$$

In addition, all elements on the right-hand side of Eq. (1) are very difficult to calculate. We use the following approximation to simplify these elements [17]–[18].

(2) Derivation of Approximate Risk Formula

(2-1) Approximation of Asset Value

The asset value is approximated in terms of the risk impact in the risk matrix, as shown in Fig. 2. Thus, the asset value is considered to be the risk impact. The degree of risk impact is defined as anywhere from 1 (low) to 5 (high). As a further approximation, these values are mapped as risk impact in a risk matrix. As shown in Fig. 2, the risk impact of the risk matrix is divided into two. For simplicity, the maximum risk impact (5) is approximated to the higher of the two divisions.

Similarly, the minimum risk impact (1) is approximated to the lower of the two.

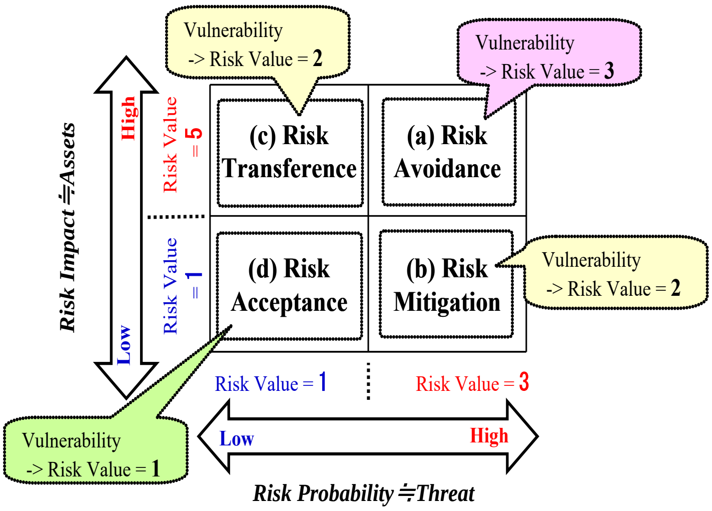


Figure 2 Risk value approximation of risk matrix.

(2-2) Approximation of Threat Value

The threat value of Eq. (1) is approximated in terms of the risk probability in the risk matrix. On the basis of references, the risk probability is defined to range from 1 (low) to 3 (high). These values are mapped to the risk probability of the risk matrix in Fig. 2, as well as the above-mentioned degree of risk probability approximation. That is, the maximum risk probability (3) is approximated to the higher of the two divisions, and the minimum (1) is approximated to the lower of the two.

(2-3) Approximation of Value of Vulnerability

The vulnerability evaluation is defined on a three-level scale: 3 (High), 2 (Medium), and 1 (Low). These levels are approximated in accordance with the classification of the risk matrix in Fig. 2. The four domains shown in the figure are classified into three categories in accordance with the risk probability and risk impact: Risk Avoidance cases are approximated to 3 (High), Risk Transference and Risk Mitigation cases to 2 (Medium), and Risk Acceptance cases to 1 (Low).

(2-4) Approximate Risk Formula

By approximating (2-1)–(2-3), Eq. (1) can be approximated to Eq. (2). In addition, the approximate value of each parameter of Eq. (2) is shown in Table 4.

$$\textit{Risk value} \fallingdotseq \textit{risk impact} \times \textit{risk probability} \times \textit{vulnerability} \tag{2}$$

Table 4: Approximate value of each parameter of Eq. (2).

	Risk Impact	Risk probability	Vulnerability	
High	5	3	Risk Avoidance	3
Low	1	1	Risk Transference and Risk Mitigation	2
			Risk Acceptance	1

3.3.2 *Calculation of Risk Value*

First, we calculated the risk values before the countermeasure by using Eq. (2). Next, the risk values after carrying out the proposed countermeasures in Table 3 were also calculated by using Eq. (2). These results are listed in Table 5.

Table 5: Risk value before and after countermeasures.

No	Risk Factor	Asset = Risk Impact	Threat = Probability	Vulnerability		Value of Risk	
				Before Counter-measure	After Counter-measure	Before Counter-measure	After Counter-measure
1	1.1.1 Access of work files with personal devices	5	1	2	1	10	5
2	1.1.2 Use of work devices for personal use	1	1	1	1	1	1
3	1.1.3 Access of unapproved sites, comsumer apps, emails	1	1	1	1	1	1
4	1.1.4 Non-compliance with security practices	5	1	2	1	10	5
5	1.1.5 Leaving confidential documents unattended	5	1	2	1	10	5
6	1.1.6 Leaving devices unattended	5	1	2	1	10	5
7	1.1.7 Sharing of computer and devices	1	3	2	1	6	3
8	1.1.8 Use of unsecured Wi-Fi communications	1	3	2	1	6	3
9	1.2.1 Device loss or theft	5	3	3	2	45	30
10	1.2.2 Shoulder hacking	1	3	2	1	6	3
11	1.2.3 Intruders gaining access to sensitive information	5	1	2	1	10	5
12	1.2.4 Eavesdropping attacks	5	1	2	1	10	5
13	2.1 Inadequate work-life balance	1	3	2	1	6	3
14	2.2 Lone working	5	3	3	2	45	30
15	2.3 Invasion of personal space due to office-related work	5	3	3	2	45	30
16	2.4 General health and safety hazards	5	1	2	1	10	5
17	2.5 Change in working habits	5	3	3	2	45	30
18	2.6 Inadequate resources	1	3	2	1	6	3
19	2.7 Lack of face-to-face communication	1	3	2	1	6	3
20	2.8 Lack of self-motivation and encouragement	1	1	1	1	1	1
Total						289	176

3.3.3 *Results of Evaluation*

As indicated in Table 6, we could reduce the risk rate by about 40% by applying the countermeasures. These results demonstrate that the above calculation can be used to quantitatively determine the effect of a countermeasure against the risks of mobile workers.

Table 6: Summarization of evaluation results.

	Before risk countermeasures (1)	After risk countermeasures (2)
Risk value (total)	289	176
Risk value reduction rate = ((1)-(2))/ (1)		0.39

4 Portfolio of Risk Countermeasures for Mobile Workers

In general, it makes sense to implement risk countermeasures in stages in view of their cost-effectiveness. In this section, we propose a portfolio (priority) of risk countermeasures based on the Computer Security Incident Response Team (CSIRT) risk countermeasure classification [19]–[20]. The CSIRT classifies risk countermeasures into three categories: Proactive Service, Reactive Service, and Security Quality Management Services. Proactive Service and Security Quality Management Service are classified as pre-countermeasures, and are given a higher priority in the introduction of countermeasures than Reactive Service.

As the proposed portfolio of risk countermeasures clearly identifies Proactive Service, Security Quality Management Service, and Reactive Service for each countermeasure, the measures can be introduced step-by-step.

4.1 Risk Mitigation

The main countermeasures in Risk Mitigation are to implement strong passwords, multi-factor authentication tools, and session security settings. Operational measures, such as avoiding the use of public Wi-Fi, should also be taken if appropriate security measures are not in place.

Next, the Risk Mitigation portfolio is presented. As shown in Table 7, out of six risk factors, Proactive Service and Security Quality Management Service, which are precautionary measures, totaled four, while Reactive Service, which relates to post-cautionary measures, totaled two. From the above, we can see that about 67% of the total measures should be prioritized.

Table 7: Portfolio result of Risk Mitigation (6 risk factors).

No.	Risk Factor	Risk Classification	Proposed countermeasure	Pre	Post	Quality
7	1.1.7 Sharing of computer and devices	Risk Mitigation	Encrypt critical data. Enforce strong password, multifactor authentication tools and session security configuration.	○		
8	1.1.8 Use of unsecured Wi-Fi communications	Risk Mitigation	Avoid using public Wi-Fi, unless appropriate security measures (e.g., VPN connection) are implemented.	○		
10	1.2.2 Shoulder hacking	Risk Mitigation	Implement shoulder hacking preventive measures decided by the enterprise.	○		
13	2.1 Inadequate work-life balance	Risk Mitigation	Introduce well-balanced policies that take into account both the risks and advantages for both the company and its employees.	○		○
18	2.6 Inadequate resources	Risk Mitigation	Implement enquiries and updates on work-flow to ensure workers requirements are met.		○	
19	2.7 Lack of face-to-face communication	Risk Mitigation	Use of social tools to make employees feel involved. Develop channels that connect the workplace community.		○	

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service.

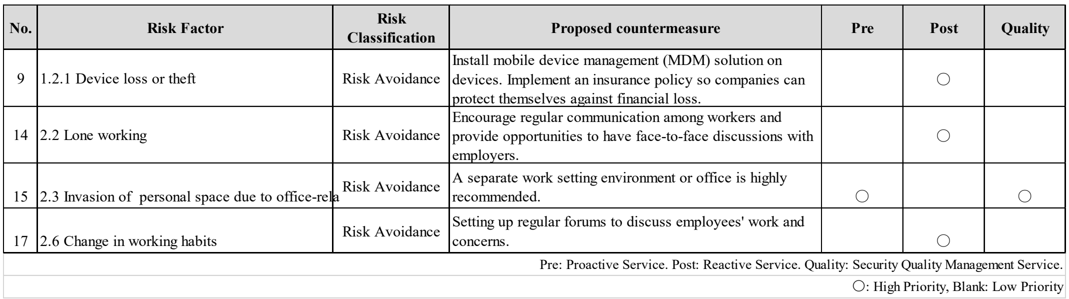
○: High Priority, Blank: Low Priority

4.2 Risk Avoidance

A key countermeasure in Risk Avoidance is the installation of a Mobile Device Management (MDM) solution on devices. From an operational point of view, it is important to promote regular communication between employees and to provide opportunities for direct discussions with employers and others.

Next, we present the portfolio of Risk Avoidance. As shown in Table 8, out of the four risk factors, there was a total of one for Proactive Service and Security Quality Management Service, which is a pre-measure, and three for Reactive Service, which refers to post-measures. From the above, we can see that about 25% of the total measures should be prioritized.

Table 8: Portfolio result of Risk Avoidance (4 risk factors).



No.	Risk Factor	Risk Classification	Proposed countermeasure	Pre	Post	Quality
9	1.2.1 Device loss or theft	Risk Avoidance	Install mobile device management (MDM) solution on devices. Implement an insurance policy so companies can protect themselves against financial loss.		○	
14	2.2 Lone working	Risk Avoidance	Encourage regular communication among workers and provide opportunities to have face-to-face discussions with employers.		○	
15	2.3 Invasion of personal space due to office-rela	Risk Avoidance	A separate work setting environment or office is highly recommended.	○		○
17	2.6 Change in working habits	Risk Avoidance	Setting up regular forums to discuss employees' work and concerns.		○	

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service.

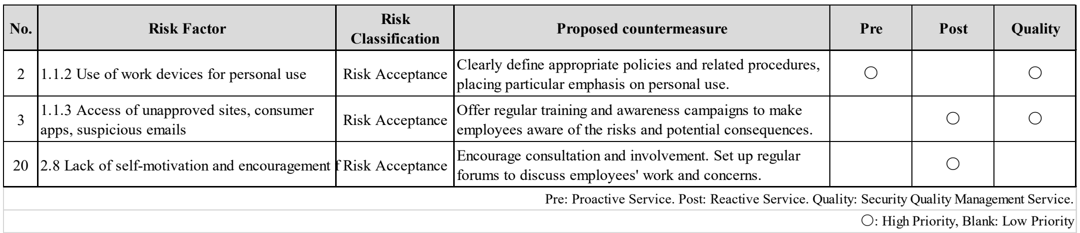
○: High Priority, Blank: Low Priority

4.3 Risk Acceptance

The main countermeasure in Risk Acceptance is to clearly define appropriate policies and relevant procedures, with a particular focus on personal use. On the operational side, regular training and awareness-raising activities should be carried out to make employees aware of the risks and potential consequences.

Next, we present the portfolio of Risk Acceptance. As shown in Table 9, out of the three risk factors, there were a total of two for Proactive Service and Security Quality Management Service, which are pre-measures, and two for Reactive Service, which refers to post-measures. From the above, we can see that about 67% of the total measures should be prioritized.

Table 9: Portfolio result of Risk Acceptance (3 risk factors).



No.	Risk Factor	Risk Classification	Proposed countermeasure	Pre	Post	Quality
2	1.1.2 Use of work devices for personal use	Risk Acceptance	Clearly define appropriate policies and related procedures, placing particular emphasis on personal use.	○		○
3	1.1.3 Access of unapproved sites, consumer apps, suspicious emails	Risk Acceptance	Offer regular training and awareness campaigns to make employees aware of the risks and potential consequences.		○	○
20	2.8 Lack of self-motivation and encouragement f	Risk Acceptance	Encourage consultation and involvement. Set up regular forums to discuss employees' work and concerns.		○	

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service.

○: High Priority, Blank: Low Priority

4.4 Risk Transference

The main countermeasures in Risk Transference are the setting up of a virtual desktop infrastructure (VDI) or mobile device management protocols. Another effective measure is enhanced network monitoring.

Next, we present the portfolio of Risk Transference. As shown in Table 10, out of the seven risk factors, there were a total of four for Proactive Service and Security Quality Management Service, which are pre-measures, and three for Reactive Service, which refers to postmeasures. From the above, we can see that about 57% of the total measures should be prioritized.

Table 10: Portfolio result of Risk Transference (7 risk factors).

No.	Risk Factor	Risk Classification	Proposed countermeasure	Pre	Post	Quality
1	1.1.1 Access of work files with personal, non-IT	RiskTransference	Setting up a virtual desktop infrastructure (VDI) or mobile device management protocol to separate company data from personal data.	○		○
4	1.1.4 Non-compliance with security practices	RiskTransference	Actively involve employees in defining and monitoring the security of company assets.	○		
5	1.1.5 Leaving confidential documents unattended	RiskTransference	Educate and train employees on standards, guidelines, and procedures for handling companys' documents.	○		
6	1.1.6 Leaving devices unattended	RiskTransference	Utilize computer locks, device management applications, and suites to help secure business data.	○		
11	1.2.3 Intruders gaining access to sensitive inform	RiskTransference	Perform continuous network monitoring using advanced and up-to-date technology.		○	
12	1.2.4 Eavesdropping attacks	RiskTransference				
16	2.4 General health and safety hazards	RiskTransference	Implement regular monitoring and enquiries to make sure employees are following safe practices.		○	

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service.

○: High Priority, Blank: Low Priority

4.5 Discussion

Lack of compliance and/or negligence on the part of the workers is a major source of risk to a company's assets and can cause significant financial and reputational damage to the company. These risks can be countered by prioritizing cybersecurity training and educating employees about risky behaviors and the potential consequences of a data breach for the workers, the company, and its customers.

Companies must also make an effort to communicate effectively with their mobile workers; consultations and involvement should be encouraged. Companies are also encouraged to equip themselves with up-to-date technologies to avoid the risk of intrusion. Using device management solutions can help with data segregation, securing emails, securing corporate documents on devices, and so on.

5 Conclusion and Future Work

In this paper, we described our risk assessment of mobile workers through a literature review of past research. First, we defined and discussed the current issues related to mobile workers. Next, we performed a risk assessment of the mobile workers using a risk management method.

We extracted a total of 20 risk factors and then proposed and classified countermeasures using the risk matrix method. Further, risk values were introduced for use in an ISMS quantitative evaluation for detailed risk assessment. The results of this evaluation clearly showed that the proposed countermeasures can reduce risks by about 40%. Finally, from a practical viewpoint, a portfolio of the proposed risk countermeasures was clearly indicated to enable the gradual introduction of risk counter-measures based on priority, which entails starting with pre-countermeasure services such as Proactive Service and the Security Quality Management Service.

Future works include the consideration of measures to address the inner life of people, particularly from a psychological perspective, in relation to the lack of work-life balance.

Acknowledgement

This work was supported by JSPS KAKENHI Grant Number JP 19H04098.

References

[1] Mitrefinch, Benefits of Mobile workforce; https://mitrefinch.com/blog/10-benefits-of-a-mobile-workforce.

[2] G. Luk, Global Mobile Workforce Forecast Update 2016-2022; https://www.strategyanalytics.com/strategy-analytics/news/strategy-analytics-press-releases/2016/11/09/the-global-mobile-workforce-is-set-to-increase-to-1.87-billion-people-in-2022-accounting-for-42.5-of-the-global-workforce.

[3] S. Tanimoto, et al., "Concept Proposal of Multi-layer Defense Security Countermeasures Based on Dynamic Reconfiguration Multi-Perimeter Lines," NBiS-2019 (ADPNA2019), AISC 1036, pp. 413–422.

[4] S. Makinen, Mobile work and its challenges to personal and collective information management, http://informationr.net/ir/17-3/paper522.html#all2004.

[5] iPass, 2018 Mobile Security Report, https://www.ipass.com/wp-content/uploads/2018/03/iPass-Mobile-Security-Report-2018.pdf.

[6] Helpnetsecurity, Apricorn; https://www.helpnetsecurity.com/2018/06/15/securing-mobile-workers.

[7] Cisco System, Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior; https://www.cisco.com/c/dam/global/en_ca/assets/pdf/Understanding_Remote_Worker_Security_A_survery_of_User_Awareness_vs_Behaviour.pdf.

[8] S. Shagvaliyeva and R. Yazdanifard, Impact of Flexible Working Hours on Work-Life Balance, American Journal of Industrial and Business Management, Vol. 4 No. 1, pp. 20-23.

[9] Boswell, W., & Olson-Buchanan, J., The Use of Communication Technologies After Hours: The Role of Work Attitudes and Work-Life Conflict, Journal of Management, 33(4), pp.592-610, 2007.

[10] J. Mulki, et al., Set up remote workers to thrive, MIT Sloan Management, pp.63-69, 2009 https://www.researchgate.net/profile/Felicia_Lassk/publication/264844669_Set_Up_Remote_Workers_to_Thrive/links/542ec3900cf29bbc126f5601.pdf.

[11] Project Management Institute, A guide to the project management body of knowledge PMBOK Guide, Sixth Edition.

[12] T. Dechen, et al., A Preliminary Study of Risk Assessment of Mobile Workers for Improvement of Work-Life Balance, The 10th International Workshop on Networking, Computing, Systems, and Software (NCSS-10), 196, 2019

[13] T. Dechen, et al., Risk Management of Mobile Workers based on Multiple Viewpoints, 9th International Congress on Advanced Applied Informatics (AAI2020), pp.649-654, 2020.

[14] Cox's risk matrix theorem and its implications for project risk management, [Online]. Available from:
http://eight2late.wordpress.com/2009/07/01/cox%E2%80%99s-risk-matrix-theorem-and-its-implications-for-project-risk-management/

[15] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, and A. Kanai, Risk Management on the Security Problem in Cloud Computing, IEEE/ACIS CNSI 2011, Korea.

[16] ISMS Risk Assessment Manual v1.4, [Online]. Available from: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ISMS%20Risk%20Assessment%20Manual%20v1.4.pdf, 2015.1.4.

[17] S. Tanimoto, et al., “A Study of Risk Assessment Quantification in Cloud Computing,” 8th International Workshop on Advanced Distributed and Parallel Network Applications (ADPNA-2014), pp. 426-431, Sep. 2014.

[18] S. Tanimoto, et al., Risk Assessment Quantification of Ambient Service, ICDS 2015: The Ninth International Conference on Digital Society, pp. 70-75, Lisbon, Feb. 2015.

[19] J.Wiik, et al., Effectiveness of Proactive CSIRT Services, In 18th Annual FIRST Conference on Computer Security Incident Handling, 2006

[20] Y. Kenmoku, et al., A Study of Assurance Level in Information Security Management - LoA Introducing Method for CSIRT Deployment -, 6th International Conference on Project Management (ProMAC 2012), 2012