International Journal of Service and Knowledge Management
International Institute of Applied Informatics
2022, Vol. 6, No. 1, IJSKM678

Risk Assessment Quantification for Bring Your Own Device Based on Practical Viewpoints

Teruo Endo [*], Shigeaki Tanimoto [†], Motoi Iwashita [†],
Toru Kobayashi [‡], Hiroyuki Sato [§], Atsushi Kanai [**]

Abstract

In recent years, the companies which introduce Bring Your Own Device (BYOD) which utilizes a personal smart phone and tablet for business are increasing in number. However, there are risks, such as information leakage of business information, an employee's personal information, etc., for the private terminal utilization instead of business use. These risks were exhaustively identified in our previous study, but based on qualitative assessment results. In order to make risk countermeasures more realistic, further quantitative evaluation is needed. Therefore, in this paper, we have added new cost risk factors for BYOD from a practical viewpoint to the risk analysis results of previous study. Furthermore, based on the results, a quantitative evaluation was conducted to verify its effectiveness. For the evaluation, the risk factor values were estimated using a risk calculation formula used in the field of information security management systems (ISMS). Thus, the combined effect of the BYOD risk measures proposed in the previous study and the cost risk measures added in this study clarified that it was possible to reduce the risk by about 56%. The results of this quantitative risk assessment are expected to help make the future use of BYOD safer and secure for companies.

Keywords: BYOD, Risk Assessment, Risk Breakdown Structure, Risk Matrix, Risk Value

1 Introduction

In recent years, the technology of personal mobile devices has advanced rapidly, especially smart phones. Smartphones can now be used not only for phone calls and e-mails, but also for installing applications and adding and deploying functions according to one's preferences. In other words, it has the functions of both a personal computer and a mobile phone. With the rapid proliferation of smartphones, more and more companies are introducing Bring Your Own Device (BYOD), which allows individuals to use their own smartphones for business purposes [1]. In

[*] Osaka Shoin Women's University, Osaka, Japan
[†] Chiba Institute of Technology, Chiba, Japan
[‡] Nagasaki University, Nagasaki, Japan
[§] The University of Tokyo, Tokyo, Japan
[**] Hosei University, Tokyo, Japan

order to prevent the spread of the new coronaviruses, teleworkers will be required to work from home in 2020, which will further increase the opportunities for the use of BYOD.

The purpose of BYOD in a company is to provide an environment where people can work anytime, anywhere, and the productivity and speed of work can be changed by making full use of the environment. In addition, the introduction of new devices and services is also intended to provide an opportunity for new ways of working and new businesses to be born.

However, there is a major security problem with BYOD because it uses private smartphones rather than business phones. Specifically, security risks include the leakage of business data, trade secrets, and employees' personal information. For example, when business data are stored in a personally owned smartphone, all of the data are managed by an individual. Therefore, in case of loss or theft, if individuals do not have passwords and security locks set up, confidential corporate information as well as personal information may be compromised [2]. Thus, with BYOD, there are various risks such as the risk of leakage of confidential information from the company side and the possibility of privacy information being leaked to the company etc. from the employee side.

In this paper, at first, we added new risk factors such as cost overrun of BYOD implementation from a more practical point of view to the results of the risk assessment in previous study [3]. Next, we evaluated the effectiveness of these risk assessment results by quantitative evaluation with risk values. As a result of these, the combined effect of the BYOD risk measures proposed in the previous study and the cost risk measures added in this study clarified that it was possible to reduce the risk by about 56%. The results of this quantitative risk assessment will contribute to the safe and secure implementation of BYOD.

2 Related Trends

2.1 Telework

Due to changes in the environment, such as the rapid spread of PCs and smartphones, and the development of high-speed broadband and public wireless LANs, anyone can easily access the Internet from anywhere [4]–[5]. Against this backdrop, many companies have introduced "telework" that enables employees to perform their work without being in the office. If companies can connect their computers and smartphones to the office and work away from the office, they will be able to work at home while raising children and doing household chores, enabling them to hire more workers.

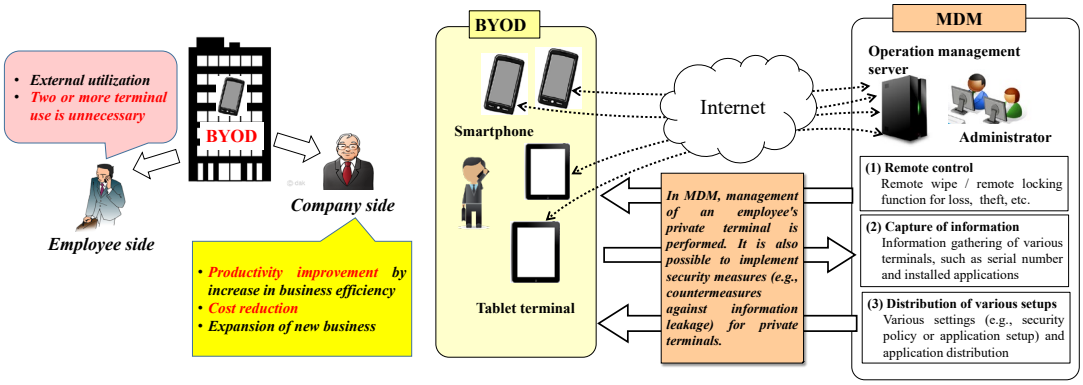
In general, there are three types of teleworkers: the satellite type, which is performed at other branches and offices other than the home office; the home type, which is performed at employees' homes; and the mobile type, which is performed while traveling by car or train. In addition, there are two types of BYOD for employees who work outside the company, one is the case where the company supplies PCs and smartphones, and the other is the case where employees use their own devices. In the latter case, BYOD requires strict management with the introduction of MDM (Mobile Device Management) and other measures to prevent confidential internal information from leaking from employees' private devices [6].

2.2 BYOD

BYOD means that employees bring their own smartphones, tablets, and personal computers to use at work. Among them, smartphones are rapidly becoming the most popular because they are

easy to carry, can be easily connected to the Internet anywhere, have an easy-to-view screen, a touch interface, and various applications.

It is also possible to access corporate information systems from smartphones and other devices used in daily life to view and input necessary information. Smartphones and tablets have become remarkably popular among individuals, and their use is expected to expand in the business field as well, with BYOD bringing changes to work time and organization. In addition, the benefits of each stakeholders in BYOD are also known, as shown in Figure 1 (1).



(1) Benefits of BYOD by Stakeholder (2) Managing BYOD with MDM

Figure 1: Relationship between BYOD and MDM

2.3 MDM

MDM is a system for managing mobile devices such as PCs, tablets, and smartphones that enables the devices to be remotely locked, thus preventing information leakage when they are lost. Companies are encouraged to use MDM to manage devices for external use and even personal devices such as those used for BYOD [6]. Figure 1 (2) shows the relationship between BYOD and MDM.

3 BYOD Risk Assessment

In general, risk assessment is conducted in the order of (1) risk identification, (2) risk analysis, and (3) risk evaluation [7]. We have conducted qualitative risk assessment in our previous study [3]. In this paper, a new risk assessment and quantification from a practical point of view are added to our previous study [3].

3.1 BYOD Risk Identification

We comprehensively extracted the risk factors of BYOD from the viewpoint of the mutually exclusive and collectively exhaustive (MECE) principle. Specifically, the risks of BYOD are divided into the corporate side and the employee side, and each is extracted comprehensively and systematically in terms of people (operation), goods (system), and money (cost). Here, risk factors were extracted using the Risk Breakdown Structure (RBS) method [8], which is commonly used as a risk management method.

As shown in Table 1, the risk factors of BYOD were divided into the corporate side and the employee side at the first level, and classified into the operational side, the system side, and the cost side at the second level. Furthermore, in the third level, 31 risk factors were extracted with reference to the results of a questionnaire on the risks felt when BYOD was introduced [9].

Table 1: Results of risk factor extraction in BYOD

No.	Level 1	Level 2	Level 3 (Risk factor)	Details of Risk Factor
1	1. Company-side	1.1 Operation	1.1.1 Off-the-job management	Problems with managing private devices outside of work hours
2			1.1.2 External management	Management issues such as how to use the device outside the company
3			1.1.3 Communication-charges responsibility of BYOD terminal	The issue of managing work outside of regular working hours
4			1.1.4 Employees' working-hours management	Issues that could lead to the release of personal information from employees' devices
5			1.1.5 An employee's personal information management	The problem of potential incidents from various unauthorized access via BYOD
6		1.2 System	1.2.1 Unauthorized access via BYOD	Private data on employees' computers mixed with business data
7			1.2.2 An employee's private data mixture in a BYOD terminal	Problems with potential exposure of confidential sales and internal data via BYOD
8			1.2.3 The leak-of-information issue of in-company confidential information	Problems that could lead to the installation of malware and virus infections via BYOD
9			1.2.4 Computer virus infection by unsuitable software etc.	The issue of security policy changes and the need to train employees due to BYOD implementation
10			1.2.5 Decision and education of the security policy of BYOD introduction	Issues that may be connected via BYOD for non-corporate business purposes etc.
11			1.2.6 URL connection destination restrictions of BYOD	The implementation and maintenance costs required to implement MDM
12		1.3 Cost	1.3.1 Security software costs	The cost of installing and maintaining the security software required for BYOD implementation
13			1.3.2 Internal infrastructure upgrade costs	Cost of change to the internal network and other systems as a result of BYOD implementation
14			1.3.3 Help desk costs	Cost of contacting employees and other users with BYOD
15			1.3.4 Compensation costs in the event of a breach of company and customer information	Credit recovery and apology costs in the event of a breach of company and customer information via BYOD
16			1.3.5 Cost of establishing a security system	The cost of expanding and maintaining the new security system as a result of BYOD implementation
17	2. Employee side	2.1 Operation	2.1.1 The installation risk of unsuitable applications to BYOD	Problems with employees potentially installing rogue software on BYOD devices
18			2.1.2 Risk of working hours becoming irregular	Problems with the introduction of BYOD and the possibility of performing work outside of regular working hours
19			2.1.3 Loss and theft of BYOD	Potential misuse issues due to lost and stolen BYOD devices
20			2.1.4 Access to unsuitable sites by BYOD	Issues that could lead to access to unauthorized sites via BYOD
21		2.2 System	2.2.1 Data leakage risk from BYOD during cloud use	The issue of potential corporate data exposure when using the cloud via BYOD
22			2.2.2 Shoulder hacking of BYOD by others	Problems with potential for shoulder hacking and other prying eyes when using BYOD outside the company
23			2.2.3 Leak of information during connection to public Wi-Fi environment etc.	Vulnerable public WiFi connections when using BYOD outside the office, which could lead to information leakage and other problems
24			2.2.4 The pass code of BYOD is not set up	Passcode lock is not set on BYOD devices, which could be misused by outsiders
25			2.2.5 Use of BYOD by family etc.	Issues that could lead to acquaintances and family members using employees' BYOD devices
26		2.3 Cost	2.3.1 Handset costs	The problem of having to pay the full cost of purchasing a device when using BYOD devices for business
27			2.3.2 Calling charges	The issue of call rates for business calls on BYOD devices
28			2.3.3 Packet charges	Packet charges for business data communication on BYOD devices
29			2.3.4 Electricity charges when charging	The issue of electricity requirements for business use on BYOD devices
30			2.3.5 Security software fees	The cost of installing and maintaining the security software required for BYOD devices
31			2.3.6 After-hours spur-of-the-moment responses	The cost of unexpectedly needing to respond to customers and others after hours

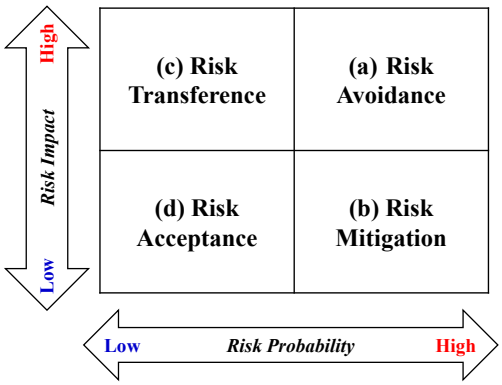
3.2 BYOD Risk Analysis

3.2.1 Risk analysis using a risk matrix

Next, the results of the risk analysis for the risk factors extracted in Table 1 are presented. With regard to risk analysis methods, the main methods are the decision-tree-based and risk-matrix methods, the former based on a quantitative perspective and the latter on a qualitative perspective

[10] - [11]. In this paper, we use a risk matrix method suitable for desk review to predict new security issues such as information leak protection in the use of BYOD in companies.

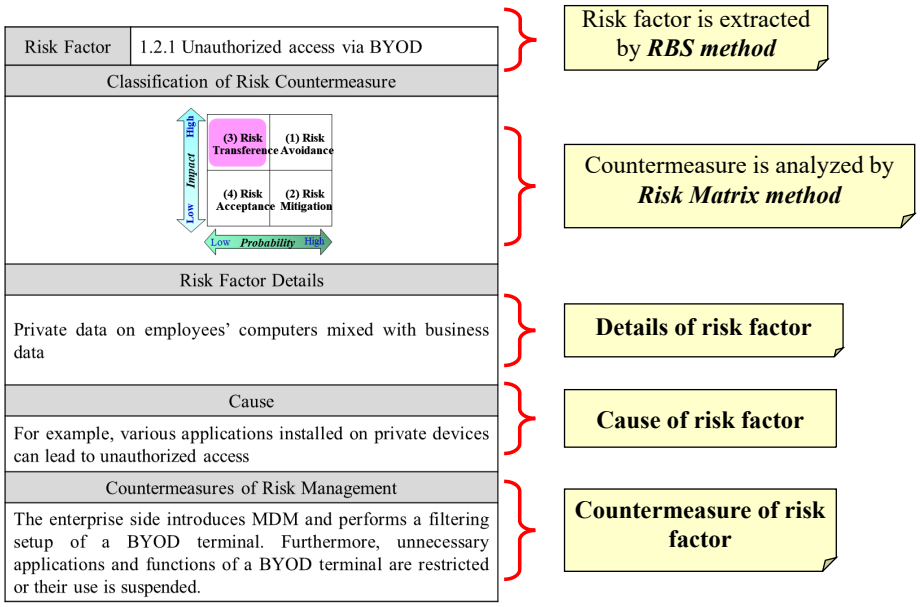
As shown in Fig. 2 (1), the risk matrix method classifies the risks into four categories: Risk Avoidance, Risk Mitigation, Risk Acceptance and Risk Transference, depending on the Risk Probability and the Risk Impact. Furthermore, based on this risk matrix method, a risk analysis is conducted using the template in Fig. 2 (2). The results of the analysis using this template for the 31 risk factors extracted in Table 1 are shown in Table 2.



(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.

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

(1) Risk Matrix: 2-dimensional analysis



(2) Template of Risk Analysis

Figure 2: Risk matrix method and analysis template

Table 2: Proposed measures to address the main risk factors in BYOD

No.	Level 1	Level 2	Level 3 (Risk Factor)	Risk Probability	Risk Impact	Risk Analysis	Proposed Countermeasures
1	1. Company-side	1.1 Operation	1.1.1 Off-the-job management	L	H	Risk Transference	MDM is installed into the private terminal (BYOD) owned by an employee. This ensures batch management, such as use restrictions of the private terminal for BYOD.
2			1.1.2 External management	L	H	Risk Transference	
3			1.1.3 Communication-charges responsibility of BYOD terminal	H	H	Risk Avoidance	The enterprise side decides on the burden share rule for BYOD communication charges.
4			1.1.4 Employees' working-hours management	L	H	Risk Transference	Use restrictions of a BYOD terminal are set on the basis of the labor standards of an enterprise.
5			1.1.5 An employee's personal information management	H	L	Risk Mitigation	The enterprise side installs MDM and restricts access of a BYOD terminal. This prevents information leakage.
6		1.2 Sysem	1.2.1 Unauthorized access via BYOD	L	L	Risk Acceptance	The enterprise side introduces MDM and performs a filtering setup of a BYOD terminal. Furthermore, unnecessary applications and functions of a BYOD terminal are restricted or their use is suspended.
7			1.2.2 An employee ' s private data mixture in a BYOD terminal	L	H	Risk Transference	Enterprise data is managed on a dedicated site that strengthens authentication and prevents company data from mixing with an employee's private data.
8			1.2.3 The leak-of-information issue of in-company confidential information.	L	H	Risk Transference	MDM is installed in the private terminal (BYOD) owned by an employee. This ensures batch management, such as use restrictions of the private terminal for BYOD.
9			1.2.4 Computer virus infection by unsuitable software etc.	H	L	Risk Mitigation	
10			1.2.5 Decision and education of the security policy of BYOD introduction	H	L	Risk Mitigation	Security policy for BYOD introduction is decided. Furthermore, employee education is performed periodically.
11			1.2.6 URL connection destination restrictions of BYOD	H	L	Risk Mitigation	MDM is installed and URL connection destinations are restricted on the basis of the security policy of a company.
12		1.3 Cost	1.3.1 Security software costs	H	L	Risk Mitigation	Mitigation through use of the cloud.
13			1.3.2 Internal infrastructure upgrade costs	H	L	Risk Mitigation	Mitigation through use of SDN and cloud computing.
14			1.3.3 Help desk costs	H	L	Risk Mitigation	Outsourcing instead of operating in-house.
15			1.3.4 Compensation costs in the event of a breach of company and customer information	L	H	Risk Transference	Insurance coverage.
16			1.3.5 Cost of establishing a security system	H	L	Risk Mitigation	Reduction by outsourcing.
17	2. Employee side	2.1 Operation	2.1.1 The installation risk of unsuitable applications to BYOD	H	L	Risk Mitigation	MDM restricts the installation range of the application to BYOD.
18			2.1.2 Risk of working hours becoming irregular	H	H	Risk Avoidance	By means of access log management, employees are careful not to exceed contracted hours.
19			2.1.3 Loss and theft of BYOD	L	H	Risk Transference	The location of BYOD is specified by the GPS function of MDM, and data is eliminated remotely.
20			2.1.4 Access to unsuitable sites by BYOD	L	H	Risk Transference	MDM restricts access of BYOD and blocks unsuitable sites from being visited.
21		2.2 System	2.2.1 Data leakage risk from BYOD during cloud use	L	H	Risk Transference	Only the cloud service aligned with the security policy of an enterprise is used.
22			2.2.2 Shoulder hacking of BYOD by others	L	L	Risk Acceptance	The shoulder hacking preventive measures (e.g., shoulder hacking prevention seal) decided by the enterprise are performed.
23			2.2.3 Leak of information during connection to public Wi-Fi environment etc.	L	H	Risk Transference	There is no connection unless Wi-Fi is aligned with the security policy of the enterprise.
24			2.2.4 The pass-code of BYOD is not set up	L	L	Risk Acceptance	Setting up a BYOD passcode is imposed by the security policy of an enterprise.
25			2.2.5 Use of BYOD by family etc.	L	L	Risk Acceptance	No relatives can use BYOD. Company data is protected by a pass code lock.
26		2.3 Cost	2.3.1 Handset costs	H	L	Risk Mitigation	Company reimburses for expenses.
27			2.3.2 Calling charges	H	L	Risk Mitigation	Company pays for/provides wireless router
28			2.3.3 Packet charges	H	L	Risk Mitigation	Company pays for/provides wireless router
29			2.3.4 Electricity charges when charging	H	L	Risk Mitigation	Company reimburses for expenses.
30			2.3.5 Security software fees	H	L	Risk Mitigation	Company reimburses for expenses.
31			2.3.6 After-hours spur-of-the-moment responses	H	H	Risk Avoidance	Benefits are converted into hours of work and then paid.

3.2.2 Characteristics of the proposed risk management plan

Based on the results in Table 2, we present the characteristics of the BYOD risk measures.

(1) Risk Transference: 10 risk responses were transferred. The main countermeasure is to use services such as MDM to avoid the risk.
(2) Risk Mitigation: There were 14 risks that were reduced by countermeasures. As a countermeasure, the cost on the company side should be reduced by using cloud computing and the cost on the individual side should be borne by the company.
(3) Risk Avoidance: There were three risks that were avoided by the countermeasures. As a countermeasure, we should instill in our employee's strict observance of working hours.
(4) Risk Acceptance: There were four risks that were retained. A countermeasure is to restrict the use of password authentication.

3.3 BYOD Risk Evaluation

Next, from a more practical point of view, we visualize the effectiveness of the proposed countermeasures against the main risk factors in the use of BYOD in companies, shown in Table 2, by adding a quantitative evaluation.

3.3.1 Criteria for calculating the risk value

a) Risk formula

In general, the risk value is expressed as Eq. (1), which is commonly used in the field of ISMS [12]–[14].

$$\text{Risk value} = \text{value of asset} \times \text{value of threat} \times \text{value of vulnerability} \quad (1)$$

a-1) Approximation of asset values and threats

In order to simplify the quantification of risk measures, we approximate the asset values and threats in Eq. (1) to the risk impact and risk probability in the risk matrix, as shown in Fig. 3. In the example in Fig. 3 assumes that the asset value is risk impact and defines the risk value as 5 for high and 1 for low, referring to the literature [13]. Similarly, we approximate the threat to the risk probability and define it as 3 for high and 1 for low.

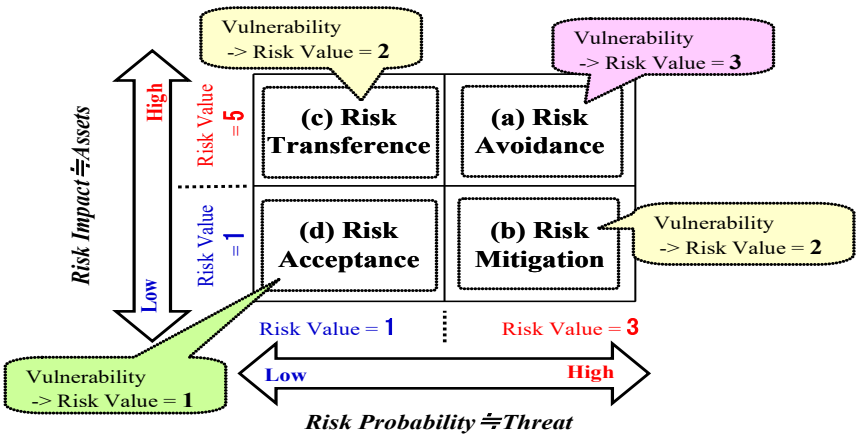


Figure 3: Approximate risk values based on the risk matrix method

a-2) Approximation of vulnerability

As in the previous section a-1), we approximate the vulnerability on a scale of 3 (high), 2 (medium), and 1 (low), referring to the reference [13]. Again, based on the evaluation of the risk matrix, we approximate that the risk equivalent of Risk Avoidance is 3 (high), Risk Transference or Risk Mitigation is 2 (medium), and Risk Acceptance is 1 (low).

b) Approximate formula for risk value

Eq. (1) can be approximated as shown in Eq. (2) by approximating the a-1) and a-2). Therefore, the risk value is calculated using this approximation equation (2).

$$\text{Risk value} = \text{risk impact} \times \text{risk probability} \times \text{value of vulnerability} \quad (2)$$

3.3.2 Results of the calculation of the risk value

a) Risk value before implementing the proposed risk measures

Based on the risk-value calculation criterion in Eq. (2), the risk values in Table 1, i.e., without the countermeasure plan shown in Table 2, are first shown in Table 3. As shown in Table 3, the total risk value before the countermeasure is 323.

Table 3: Risk values before the implementation of the proposed risk measures

No	Level 3: Risk Factors	Threat	Asset	Vulner-ability	Value of Risk
1	1.1.1 Off-the-job management	1	5	2	10
2	1.1.2 External management	1	5	2	10
3	1.1.3 Communication-charges responsibility of BYOD terminal	3	5	3	45
4	1.1.4 Employees' working-hours management	1	5	2	10
5	1.1.5 An employee's personal information management	3	1	2	6
6	1.2.1 Unauthorized access via BYOD	1	1	1	1
7	1.2.2 An employee's private data mixture in a BYOD terminal	1	5	2	10
8	1.2.3 The leak-of-information issue of in-company data of confidential information.	1	5	2	10
9	1.2.4 Computer virus infection by unsuitable software etc.	3	1	2	6
10	1.2.5 Decision and education of the security policy of BYOD introduction	3	1	2	6
11	1.2.6 URL connection destination restrictions of BYOD	3	1	2	6
12	1.3.1 Security software costs	3	1	2	6
13	1.3.2 Internal infrastructure upgrade costs	3	1	2	6
14	1.3.3 Help desk costs	3	1	2	6
15	1.3.4 Compensation costs in the event of a breach of company and customer information	1	5	2	10
16	1.3.5 Cost of establishing a security system	3	1	2	6
17	2.1.1 The installation risk of unsuitable applications to BYOD	3	1	2	6
18	2.1.2 Risk of working hours becoming irregular	3	5	3	45
19	2.1.3 Loss and theft of BYOD	1	5	2	10
20	2.1.4 Access to unsuitable sites by BYOD	1	5	2	10
21	2.2.1 Data leakage risk from BYOD during cloud use	1	5	2	10
22	2.2.2 Shoulder hacking of BYOD by others	1	1	1	1
23	2.2.3 Leak of information during connection to public Wi-Fi environment etc.	1	5	2	10
24	2.2.4 The pass code of BYOD is not set up	1	1	1	1
25	2.2.5 Use of BYOD by family etc.	1	1	1	1
26	2.3.1 Handset costs	3	1	2	6
27	2.3.2 Calling charges	3	1	2	6
28	2.3.3 Packet charges	3	1	2	6
29	2.3.4 Electricity charges when charging	3	1	2	6
30	2.3.5 Security software fees	3	1	2	6
31	2.3.6 After-hours spur-of-the-moment responses	3	5	3	45
Total					323

b) Risk value after implementing the proposed risk measures

Next, Table 4 shows the results of the calculation of risk values for the implementation of MDM and various cost mitigation measures, as shown in Table 2.In this case, the implementation of the countermeasure is assumed to result in a vulnerability of 1 (low). In general, implementing a countermeasure perfectly is not realistic. Thus, we assumed that all the vulnerabilities were decreased by one level after implementing the countermeasures.

As shown in Table 4, the risk values of 31 risk factors are calculated after the implementation of the proposed risk measures, and the total value is 141.

Table 4: Risk values after implementing the proposed risk measures

No	Level 3: Risk Factors	Threat	Asset	Vulner-ability	Value of Risk
1	1.1.1 Off-the-job management	1	5	1	5
2	1.1.2 External management	1	5	1	5
3	1.1.3 Communication-charges responsibility of BYOD terminal	3	5	1	15
4	1.1.4 Employees' working-hours management	1	5	1	5
5	1.1.5 An employee's personal information management	3	1	1	3
6	1.2.1 Unauthorized access via BYOD	1	1	1	1
7	1.2.2 An employee's private data mixture in a BYOD terminal	1	5	1	5
8	1.2.3 The leak-of-information issue of in-company confidential information	1	5	1	5
9	1.2.4 Computer virus infection by unsuitable software etc.	3	1	1	3
10	1.2.5 Decision and education of the security policy of BYOD introduction	3	1	1	3
11	1.2.6 URL connection destination restrictions of BYOD	3	1	1	3
12	1.3.1 Security software costs	3	1	1	3
13	1.3.2 Internal infrastructure upgrade costs	3	1	1	3
14	1.3.3 Help desk costs	3	1	1	3
15	1.3.4 Compensation costs in the event of a breach of company and customer information	1	5	1	5
16	1.3.5 Cost of establishing a security system	3	1	1	3
17	2.1.1 The installation risk of unsuitable applications to BYOD	3	1	1	3
18	2.1.2 Risk of working hours becoming irregular	3	5	1	15
19	2.1.3 Loss and theft of BYOD	1	5	1	5
20	2.1.4 Access to unsuitable sites by BYOD	1	5	1	5
21	2.2.1 Data leakage risk from BYOD during cloud use	1	5	1	5
22	2.2.2 Shoulder hacking of BYOD by others	1	1	1	1
23	2.2.3 Leak of information during connection to public Wi-Fi environment etc.	1	5	1	5
24	2.2.4 The pass code of BYOD is not set up	1	1	1	1
25	2.2.5 Use of BYOD by family etc.	1	1	1	1
26	2.3.1 Handset costs	3	1	1	3
27	2.3.2 Calling charges	3	1	1	3
28	2.3.3 Packet charges	3	1	1	3
29	2.3.4 Electricity charges when charging	3	1	1	3
30	2.3.5 Security software fees	3	1	1	3
31	2.3.6 After-hours spur-of-the-moment responses	3	5	1	15
Total					141

3.3.3 Results of the evaluation

Table 5 shows the results of the calculation of risk values before and after the risk measures in Tables 3 and 4. Here, Table 5 shows that the risk reduction rate is about 56% when the operational, system and cost measures are implemented as risk measures. As shown in 3.3.2 b), the vulnerability is assumed to be 1 (low) after the risk countermeasure, however, our assessment is relatively severe because the vulnerability is originally close to 0 in the ideal proposal.

Table 5: Risk Values Before and After Risk Measures

	Total risk value Σ(asset value × threat × vulnerability)
Before the risk management (a)	323
After the risk management (b)	141
Risk reduction rate: ((a)-(b)) / (a)	0.56

Table 6 categorizes the risk countermeasures proposed in this study into operations, systems, and costs, and shows the extent to which risk was reduced for each of these measures. As shown in Table 6, operational risk measures accounted for 50% of the overall risk reduction value. Next, cost-related risk measures accounted for more than 30%. Thus, it can be seen that operational and cost risk measures are important in BYOD risk measures.

As a result, the quantitative results from these risk values clarified that the effectiveness of the risk measures can be verified more specifically from the previous qualitative evaluation.

Table 6: Risk values by measure

Classification of risk measures	Reduced risk value by implementation of risk measures	Percentage of reduction risk
Operation	91	0.50
System	29	0.16
Cost	62	0.34
Total of reduced risk value	182	-

4 Conclusion

In this paper, we have quantified the risk assessment in the use of BYOD in the enterprise. In our previous study [3], we proposed a countermeasure based on the qualitative risk assessment, and here, we further verified the effectiveness of the countermeasure plan for the cost side, which we took into account in our previous study and in this paper, by quantitative evaluation using risk values. The results of the risk assessment show that the main risk of BYOD adoption is the risk of information leakage, and that the centralized management of terminals through the introduc-

tion of MDM is an effective countermeasure against this risk, which can be set up in accordance with the corporate security policy.

In addition, in terms of newly added cost risk measures, we proposed that the company should bear the cost of the BYOD environment and reduce costs through the use of cloud computing. As a result of these, the combined effect of the BYOD risk measures proposed in the previous study and the cost risk measures added in this study clarified that it was possible to reduce the risk by about 56%.

As mentioned above, it is expected that the introduction of BYOD in companies will be promoted and the convenience of BYOD will be improved for employees.

Future work includes the cost-effectiveness of specific measures, such as the introduction of MDM.

Acknowledgement

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

References

[1] ESET/Malware Information Bureau, The dangers of "BYOD", the use of personal computers and smartphones for business, KADOKAWA ASCII Research Laboratories, (in Japanese); https://ascii.jp/elem/000/002/006/2006886/

[2] Ministry of Internal Affairs and Communications, Section 2: Information Security and Safe and Secure Use, White Paper on Information and Communications 2013（PDF version）(in Japanese); https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/pdf/n3200000.pdf

[3] S. Tanimoto, S. Yamada, M. Iwashita, T. Kobayashi, H. Sato, A. Kanai, Risk Assessment of BYOD: Bring Your Own Device, 2016 IEEE 5th Global Conference on Consumer Electronics (GCCE), pp.511-514, 2016

[4] Ministry of Internal Affairs and Communications, Development of broadband infrastructure, (in Japanese); https://www.soumu.go.jp/main_sosiki/joho_tsusin/broadband/index.html

[5] Ministry of Internal Affairs and Communications, National Broadband Policy, (in Japanese); https://www.soumu.go.jp/g-ict/item/ict/index.html

[6] Myeongju Ji, Sungryong Kim, Yongjin Park, Jeong Hyun Yi, Mobile device management system with portable devices, 2015 International Symposium on Consumer Electronics (ISCE), pp.1-2, 2015

[7] K. Noguchi, Risk Management Technology to Help You Achieve Your Goals, Japanese Standards Association, 2009, (in Japanese)

[8] J. KEÇI, A User- Oriented Implementation of Risk Breakdown Structure in Construction Risk Management, 2nd International Balkans Conference on Challenges of Civil Engineering, BCCCE, ALBANIA, pp.582-593, 2013

[9] A. Ichijo, Threat of "shadow IT" secretly hitting Japanese companies, 2014, (in Japanese); https://www.itmedia.co.jp/news/articles/1404/18/news037.html

[10] Dey, P.K. Project risk management: A combined analytic hierarchy process and decision tree approach. Cost Eng. 2002, 44, 13–26.

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

[12] M. S. Toosarvandani, N. Modiri, and M. Afzali, The Risk Assessment and Treatment Approach in order to Provide LAN Security based on ISMS Standard, International Journal in Foundations of Computer Science & Technology (IJFCST), pp. 15–36, Vol. 2, No. 6, Nov., 2012

[13] H. Sato, T. Kasamatsu, T. Tamura, and Y. Kobayashi, Information Security Infrastructure, Kyoritsu Shuppan Co., Ltd., 2010, (in Japanese)

[14] ISMS Risk Assessment Manual v1.4, https://www.scribd.com/document/202271054/ISMS-Risk-Assessment-Manual-v1-4