International Journal of Service and Knowledge Management
International Institute of Applied Informatics
2024, Vol. 8, No. 1, IJSKM704

Countermeasure Portfolio Management of Silent Cyber Risks for Suitable Return of Investment

Ryuya Mishina[*], Shigeaki Tanimoto[*], Hideki Goromaru[*], Hiroyuki Sato[†], Atsushi Kanai[‡]

Abstract

In recent years, with the continuing development of the Internet of Things (IoT), various devices are now connected a huge number of networks and are being used for diverse purposes. The IoT has the potential to link cyber risks to actual property damage, as cyberspace risks are connected to physical space. With this increase in unknown cyber risks, the demand for cyber insurance is increasing. One of the most serious emerging risks is the silent cyber risk, and it is only likely to increase in the future. However, at present, security countermeasures against silent cyber risks are insufficient. In this paper, we propose a countermeasure portfolio management of silent cyber risk for organizations with the objective of contributing to the development of risk management methods against new cyber risks. Specifically, we modeled silent cyber risk by focusing on state transitions to different risks. We newly defined two types of silent cyber risk, Alteration risk and Combination risk, and conducted a risk assessment that identified 23 risk factors. After analyzing them, we found that all were classified as Risk Transference. We clarified that the most effective risk countermeasure for Alteration risk was insurance and for Combination risk was countermeasures to reduce the impact of the risk factors themselves. Our evaluation showed that the silent cyber risk could be reduced by about 50%, thus demonstrating the effectiveness of the proposed countermeasures. We also investigated the risk assessment results of silent cyber risk from the operational perspective. Specifically, we applied portfolio management based on the return on investment of risk countermeasures for silent cyber risks and found that proactive countermeasures tended to have higher priority.

Keywords: Silent cyber risk, Alteration risk, Combination risk, Risk Management, Risk Breakdown Structure, Risk Matrix, Portfolio Management

1 Introduction

In recent years, new cyber attacks such as targeted attacks against government offices, companies, and critical infrastructure providers have become increasingly sophisticated, and the damage caused by the leakage of confidential information has become enormous. As these new cyber attacks are more sophisticated than their predecessors (e.g., Emotet), the organizations taking countermeasures are not fully prepared due to their lack of expertise along with the time and cost required to provide security education [1]. In addition, with the continued development of the IoT, various devices are now connected to a vast number of

[*] Faculty of Social System Science, Chiba Institute of Technology, Chiba, Japan
[†] Information Technology Center, The University of Tokyo, Tokyo, Japan
[‡] Faculty of Science and Engineering, Hosei University, Tokyo, Japan

network sand are being utilized in diverse ways. Moreover, the IoT may cause cyber risks to become connected to physical spaces, which could lead to actual damage to property [2].

The demand for cyber insurance is increasing with the increase of new cyber risks that relate to the physical environment in addition to the traditional cyber environment. Such cyber risks are therefore considered emerging risks. However, there are many issues for insurance companies when it comes to underwriting such new cyber risks. One of the most serious emerging risks is the silent cyber risk, which is an unknown risk that is not explicitly covered or exempted by traditional property insurance policies [3]. Emerging risks include both previously unanticipated risks and risks that turn out to be much more frequent and severe than expected [4]. Silent cyber risks often surface in court cases over the availability of compensation after the actual damage has occurred, and the exposure (i.e., the degree to which assets are exposed to the risk) may increase in the future as cyber damages continue to increase and diversify [3]. However, at present, risk countermeasures against silent cyber risks have not been sufficiently studied.

In this paper, we first clarify the current status and issues of silent cyber risk on the basis of a literature review and case studies and then perform a risk management for the issue of silent cyber risk. Specifically, we extracted the risk factors of silent cyber risks for companies, analyze the risk factors, and propose countermeasures. We then evaluated the proposed countermeasures and clarify their effectiveness. To extract risk factors, we used the Risk Breakdown Structure (RBS) method, which is a risk analysis method commonly used in risk management [5]. Note that this is a qualitative method. To analyze the risk factors and proposed countermeasures, we used the risk matrix method, which is also a qualitative method and is suitable for considering countermeasures against unknown risk factors [6]. We then evaluated the proposed countermeasures using the risk values and clarified their effectiveness. Finally, we created a portfolio of proposed risk countermeasures from the viewpoint of practical applicability and clarified portfolio management for their gradual introduction. In this way, it helps to reduce the silent cyber risk, which is a new risk in the IoT society, and contribute to the construction of a safe and secure IT environment.

In the following, Section 2 of this paper clarifies the current status and issues of silent cyber risks, and Section 3 details the results of the assessment based on the risk analysis of silent cyber risks, with reference to the issues discussed in Section 2. Section 4 describes the portfolio of proposed risk countermeasures. Finally, we present our conclusions and mention future work in Section 5.

2 Current Status of Silent Cyber Risk

2.1 Overview of Silent Cyber Risk

In this section, we explain the various terms related to silent cyber risk. Silent cyber risks are defined as “cyber risks that are not explicitly covered or exempted in the terms and conditions of traditional property and casualty insurance (traditional insurance)” [3]. This is because cyber incidents can result in property damage and liability that have traditionally been covered by property and new types of insurance, and may be considered covered not only by cyber insurance designed to cover cyber risks but also by traditional insurance that does not consider cyber risks. For example, if a cyber attack on a factory causes a fire in that factory, it might be paid for by fire insurance, which is a traditional insurance policy, not cyber insurance. Silent cyber risk is also defined as “one of the emerging risks” [3].

Emerging risks or new risks (in the broad sense) are defined as "either (1) previously unanticipated risks (new risks in the narrow sense) or (2) risks that were previously anticipated but have turned out to be much more frequent or severe than expected". The opposite of emerging risk is positioned as "(3) normal risk" [4]. In addition, Swiss Re [4] defines emerging risks as "new or changed risks that are difficult to countermeasure and whose impact on the business has not been adequately considered" [4].

In this paper, on the basis of the above definitions, the terms are defined as follows.

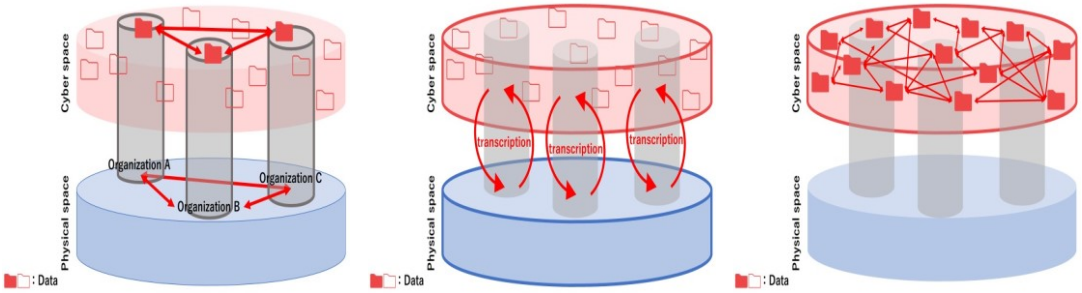
- Emerging risks are risks that include (1) and (2) above, excluding (3).
- Silent cyber risk is one form of emerging risk that includes (1) and (2), and can result in not only cyber damage but also property damage and liability.

2.2 State of Silent Cyber Risk

Silent cyber risk is often expressed in court cases regarding the availability of compensation after actual damage has occurred. In the development of cyber insurance, cyber-related exemptions have been added to the terms and conditions of conventional insurance policies, as some cases of cyber risks that were thought to be outside the scope of conventional insurance coverage have in fact been covered by conventional insurance. Moreover, cyber risk is a systemic risk, i.e., the risk that arbitrary fluctuations will spread to the entire system and exceed the limits of safety. The Petya/NotPetya attacks in 2017, for example, revealed that cyber damage can cause massive damage and disruption to a wide variety of businesses, which requires further consideration of cyber damage coverage [3][7]. One of the reasons for this is the convergence of cyber space and physical space in the digital transformation (DX) era, which is currently progressing at a rapid pace. A specific incident may spill over not only into cyber space but also into physical space, thus affecting the entire cyber-physical system (CPS) including both cyber and physical spaces and causing the entire system to malfunction.

This industrial structure, called the value creation process, consists of three layers: organization, cyberspace, and physical space, as shown in Fig. 1 [2]. In the realm of data conversion and distribution, many new components (devices, software, communication means, etc.) are being introduced, and the number of these components and the parties involved with them is increasing. In such a situation, the more the components increase, change, or fluctuate, and the more complex and difficult it is to understand the functioning principles of the components, the more easily the risk increases. The scope of responsibility of each party when an incident occurs is also less clear, and it is confusing to determine what the response should be [2][7].

According to the "Security Roundup for the First Half of 2020" report published by Trend Micro Inc. in August 2020, the average amount of damage suffered by organizations experiencing cyber damage was 147 million yen, which indicates that the threat of cyber damage is enormous [8]. In terms of the number of cyber attacks directed at domestic networks, it is estimated that there were about 500.1 billion cyber attacks in 2020 (a 3.3-fold increase in four years), and cyber attacks are increasing every year [9]. To reduce the residual risk of silent cyber risk to an acceptable level, it should be effective to share the risk by purchasing cyber insurance as a risk response option [10]. However, the number of security incidents is still increasing and security countermeasures are not always sufficient. Moreover, factors to identify all cyber risks, including new risks, have not been established yet. In other words, since the incidents caused by various cyber attacks that may occur in the future are unknown, the necessity of passing these incidents on through insurance is not understood, and the negative spiral is repeated in the process of risk management [11].



(1) Layer 1: Inter-organizational connections

(2) Layer 2 :The connection between physical space and cyber space

(3) Layer 3 : Cyberspace Connections

Figure 1: Three-tiered structure of value creation process (prepared from reference [2]).

2.3 Features of Silent Cyber Risk

In subsections 2.1 and 2.2, we defined the characteristics of silent cyber risk as those that make it difficult to recognize the risk and difficult to assess the risk. Specifically, we defined four characteristics of silent cyber risks that make them difficult to identify, as follows.

- Insufficient quantification and management of risk.
- Threats to the value creation process, which is a new supply chain that is intricately linked across both cyberspace and physical space, are different and more complex than those faced by routine and linear supply chains, and the scope of the impact of damage caused by these threats is expanding.
- There is an increased possibility that the effects of small incidents can easily spread to the entire system, and there is also an increased concern about cyber attacks through physical space.

2.4 Definition of Silent Cyber Risk

The results of the literature review [3][4][7] demonstrate that risk has various names and different states. From these results, we modeled silent cyber risk by considering the risk between different states as a state transition, as shown in Fig. 2 [12].

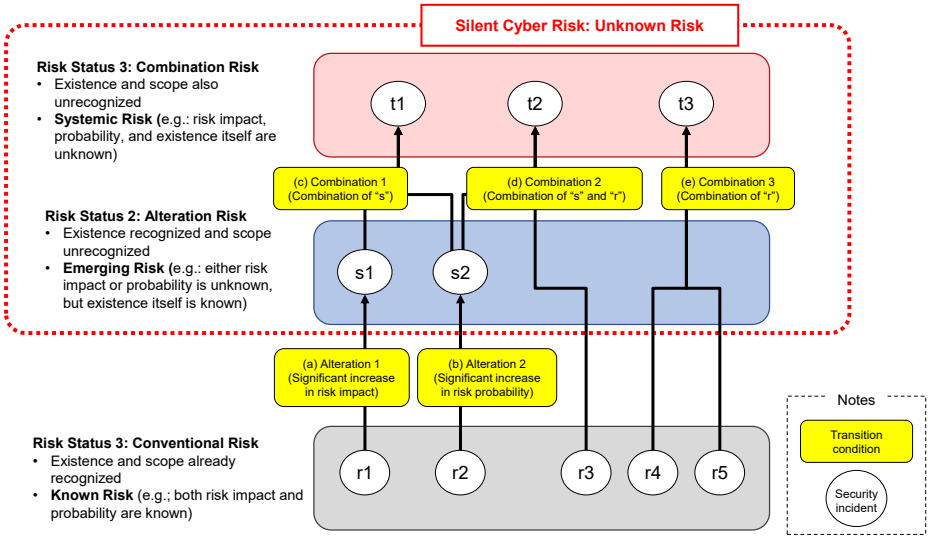


Figure 2: Modeling silent cyber risk.

Specifically, the known risk is defined as conventional risk and is designated as risk status 1. In this status, risk impact and probability are also known. Based on this risk status, the status is defined as an unknown risk as it transitions based on a variety of conditions.

First, we assume that the existing normal risk becomes a new state of risk when a transition condition that far exceeds expectations occurs, as shown in Fig. 2(a): Transition condition (significant change in risk impact) and (b): Transition condition (sudden increase in risk probability). This condition is defined as an alteration risk (emerging risk). Next, as shown in Fig. 2(c)–(e), we define combinatorial risk (systemic risk) as the status when transition conditions occur as a combination of both alteration risks (Fig. 2(c)), combination of both conventional risks (Fig. 2(e)), or a combination of conventional risk and alteration risk (Fig. 2(d)). Furthermore, we define the status of "Alteration Risk" and "Combination Risk" in Fig. 2 as "Silent Cyber Risk", which means unknown risk. As an example of silent cyber risk, Stuxnet [13] became one of the previously unknown new risks in 2010 due to the mixing of information technology (IT) systems and operational technology (OT) systems, which intersected risks from each system that had originally never met.

The validity of these models is explained below based on security incident cases that have occurred in the past.

2.4.1 Examples of Security Incidents Transitioning to Alteration Risk

The patterns of transition to alteration risk shown in Fig. 2(a) and (b) are explained in detail in Fig. 3(a), which shows the pattern of transition from conventional risk to alteration risk when the risk impact becomes significantly large, and in Fig. 3(b), which shows the pattern of transition to alteration risk when the risk occurrence probability becomes significantly larger.

Here, the symbols in parentheses ((I), (P)) in the alteration risk of risk status 2 represent the type of alteration risk. That is, Alteration Risk (I) represents the alteration risk when the risk impact of the normal risk becomes significantly larger. Similarly, Alteration Risk (P) represents the alteration risk when the risk occurrence probability of the normal risk becomes significantly larger.

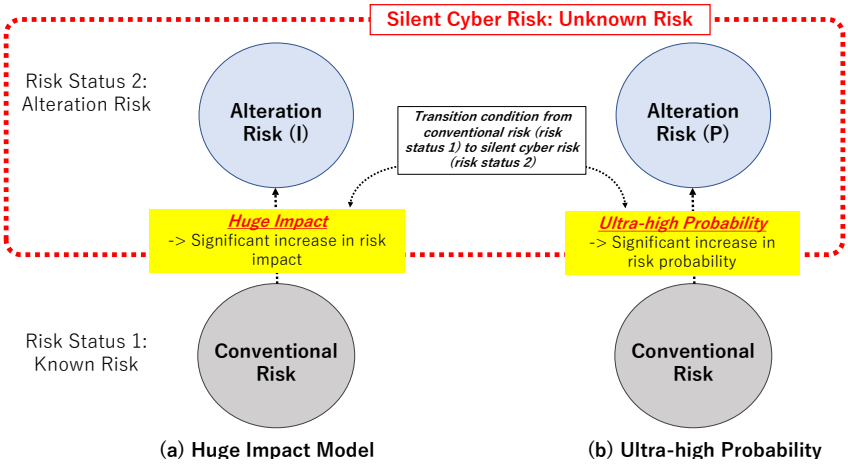


Figure 3: Alteration risk transition model.

Examples of mapping these models to real models based on past security incidents are shown in Tables 1 and 2 [14], [15]. Table 1 shows, for example, that while early malware was mainly aimed at pranks and the like, the impact has now become so severe that it has transitioned to crimes that demand money, such as ransomware. Similarly, as shown in Table 2, early DoS attacks were relatively simple, whereas today they are more complex and evolved, as evidenced by DDoS attacks

Table 1: A practical example of alteration risk (I).

Conventional Risk	Transition Conditions; Significant increase in risk impact	Alteration Risk (I)
Early-stage malware	Mischief → Crime	Ransomware
Unauthorized access (outside)	Outside the company → Inside the company	Unauthorized access (inside)

Table 2: A practical example of alteration risk (P).

Conventional Risk	Transition Conditions; Significantly greater probability of occurrence	Alteration Risk (P)
DoS attack	Increased frequency of attacks	DDoS attack
Malware	Increased sources of infection	Worm

2.4.2 Examples of Security Incidents Transitioning to Combination Risk

As shown in Fig. 4, the condition for transitioning from conventional risk to combination risk is a transition caused by a combination of multiple and heterogeneous conventional risks.

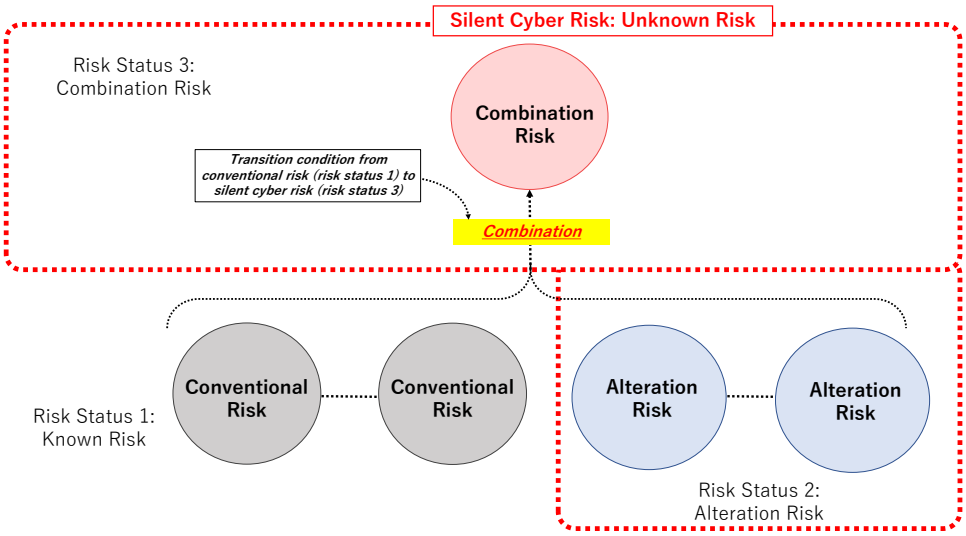


Figure 4: Combination risk transition model.

Next, to verify the effectiveness of the combinatorial risk transition model in Fig. 4, we evaluate the model based on actual security incidents that have occurred in the past. Table 3 shows an example of mapping past risks against combination risks. Here, Stuxnet [13] is an example of a nuclear power system with no Internet connection that was infiltrated internally via a USB memory stick and caused significant damage. More recently, the occurrence of internal fraud in combination with cyber risks (information leakage) and psychological risks (application of a fraud triangle (opportunity, pressure, rationalization, etc.) [16]) has become apparent.

Table 3: A practical example of combination risk.

Conventional Risk		Transition Conditions	Combination Risk
Cyber risk (Malware)	Physical risk (Unknown USB memory)	Cyber risk vs. Physical risk (IT risk vs. OT risk)	Stuxnet [13]
Cyber risk (Information leakage)	Psychological risk (Fraud triangle [16])	Cyber risk vs. Psychological risk	Internal fraud

2.4.3 Limitations of This Paper

The silent cyber risks covered in this paper are limited to three changes in known risks: 1) increased impact, 2) increased frequency of occurrence, and 3) combinations, i.e., "known-unknowns".

Risks other than these, i.e., "unknown-unknowns", are excluded. The risks associated with this type of risk need to be considered based on concepts such as offensive security [17] and MITER ATT&CK [18], and remain a topic for future work.

3 Proposed Risk Assessment for Silent Cyber Risk

In general, risk assessment consists of 1) identification of risk factors, 2) analysis of risk factors, and 3) risk evaluation. Here, we visualize the effectiveness of the proposed countermeasures by adding quantitative assessments to the main risk factors of silent cyber risks in organizations.

3.1 Risk Identification of Silent Cyber Risks

To identify risk factors, we use the risk breakdown structure (RBS) method, a typical method for risk management in project management [5]. Table 4 lists the results, where we have divided the risk factors of silent cyber risk in organizations into “Alteration risk” and “Combination risk” from an exhaustive perspective. In addition, in “Combination risk”, we define three boundaries as the areas connected to cyberspace: physical, psychological, and the environment surrounding cyberspace. In total, 23 risk factors were identified.

3.2 Risk Analysis of Silent Cyber Risks

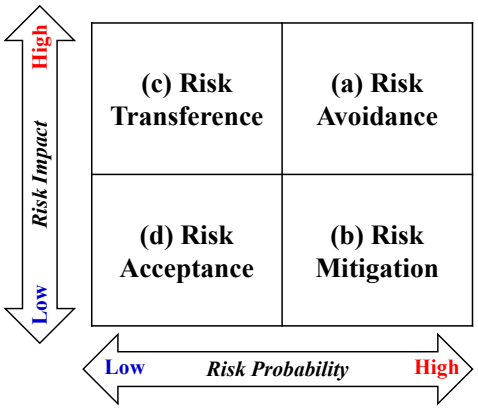
This section presents the results of our risk analysis for the risk factors of silent cyber risk in the organizations shown in Table 4 We use the risk matrix method to overview the silent cyber risk from a qualitative perspective, as the current work is a risk assessment in the initial study stage. As shown in Fig.5, the risk matrix method classifies risks into four categories: “Risk Avoidance”, “Risk Mitigation, “Risk Transference”, and “Risk Acceptance”, according to the risk probability and the risk impact, and then formulates countermeasures.

Next, we proposed risk countermeasures for the 23 risk factors of silent cyber risk in Table 4 using the risk matrix method. The results are shown in Table 5, where we can see that the countermeasures for all 23 risk factors were Risk Transference. We then investigated the features of these risk countermeasures and clarified the tendency of the risk countermeasures for each major risk factor as follows.

1) Alteration risk: It is effective to pass on the risk through insurance or other means.
2) Combination risk: Countermeasures to reduce the impact of the risk factors themselves are effective.

Table 4: List of risk factors based on RBS for silent cyber risk in organizations.

No.	Level 1	Level 2	Level 3/ Risk Factors		Contents
1	Alteration risk	Natural disasters	Earthquake		Loss of data assets due to loss and damage of hardware devices. Loss of data assets due to loss or damage of hardware.
2			Tsunami		Loss of data assets due to loss and damage of hardware devices. Loss of data assets due to loss or damage of hardware.
3			Typhoon		Loss of data assets due to loss or damage of hardware.
4			Volcanic activity		Loss of data assets due to hardware equipment failure.
5		Human factors	Pandemic		Risk of restriction of activities at overseas bases, etc. Risk of information leakage due to remote work.
6			War and terrorism		Loss of data assets due to loss and damage of hardware devices. Loss of data assets due to loss or damage of hardware.
7			Cyberterrorism		DDoS attacks that target an organization's information assets or money, business email fraud, and large-scale, urgent terrorist attacks that exploit software vulnerabilities.
8	Combination risk	Cyber ×Physical	Intra-organizational network (Fixed)	Cyber attack	DDoS attacks, business email fraud, and attacks that exploit software vulnerabilities.
9				Vulnerability of IoT devices	Increase in the number of affected people. Increased risk of viral infection.
10			Intra-organizational network (Movement)	Cyber attack	DDoS attacks, business email fraud, and attacks that exploit software vulnerabilities.
11				Vulnerability of IoT devices	Increase in the number of affected people. Increased risk of viral infection.
12			Extra-organizational networks	Supply chain vulnerabilities	Inadequate measures due to inconsistent security governance and security policies.
13				SNS	Flame wars such as defamation and malicious attacks. Sending of inappropriate information by employees.
14		Cyber ×Psychology	Fatigue	Improper internal behavior	Fraud by development, maintenance, and operation staff, and transactions that deviate from rules and norms.
15				Burnout	Loss or leakage of information assets caused by loss of motivation to work and sense of belonging.
16			Human error	Slip	Loss or damage of information assets caused by errors due to failures in the work execution phase.
17				Mistake	Loss or damage of information assets caused by errors due to misrecognition.Loss of or damage to information assets caused by errors in recognition.
18				Lapse	Loss of or damage to information assets caused by errors due to forgetting to do what needs to be done.
19				Negligence	Inadequate measures during development, inadequate measures during operation.
20		Cyber ×Environment	Legal	General Data Protection Regulation (GDPR)	Subject to sanctions under the scope of the GDPR.
21				Responsibility decomposition point	Due to unclear scope of responsibility. Inadequate security measures.
22			System	Illegal mining of virtual currency	The hijacked PC or server can be exploited and their resources used to mine virtual currency. The hijacked PC or server is then used to mine virtual currencies.
23				Artificial Intelligence (AI)	Risk of unfair consequences of legitimate (intentional) operation. The risk that learning will produce unfair results.



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 to the level at which risk can be accepted.

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

(d) Risk Acceptance: Accept a risk unconditionally.

Figure 5: Risk matrix method.

Table 5: Proposed countermeasures against risk factors of silent cyber risk.

No.	Risk Factors	Risk Probability	Risk Impact	Risk Classification	Outline of countermeasures
1	Earthquake	Low	High	Risk Transference	Take anti-vibration measures to reduce the impact of earthquakes, and store frequent backups in the cloud or other cyberspace. Measures such as insurance are effective.
2	Tsunami	Low	High	Risk Transference	Avoid locations that may be submerged in water, such as offices on two or more floors and waterproofing of hardware devices. Avoid locations where there is a risk of submersion. Also, back up frequently. Store data in cyberspace, such as in the cloud. Measures such as insurance are effective.
3	Typhoon	Low	High	Risk Transference	Consider installing an emergency power supply and make frequent backups in the cloud or other cyberspace. Store the data in cyberspace. Measures to pass on the losses through insurance are effective.
4	Volcanic activity	Low	High	Risk Transference	Use of dust-proof hardware and frequent backups. Store in cyberspace, such as in the cloud. Insurance is an effective measure.
5	Pandemic	Low	High	Risk Transference	Formulation of security policies for activities outside the office, and implementation of security education, etc. Measures to pass the cost on through insurance, etc. are effective.
6	War and terrorism	Low	High	Risk Transference	Store frequent backups in the cloud or other cyberspace. Measures to pass on the damage through insurance are effective.
7	Cyberterrorism	Low	High	Risk Transference	Acquisition of backups to prevent ransomware. It is also important to prepare a response flow for recovery, conduct training, and implement recovery tests. Measures to pass the cost on through insurance are effective.
8	Cyber attack	Low	High	Risk Transference	In addition to basic security measures, improve the attention of users. Measures to pass the cost on through insurance, etc. are effective.
9	Vulnerability of IoT devices	Low	High	Risk Transference	Check access logs and communication logs, etc., and if it can be determined that the attack is being conducted from a specific IP address, prevent access from that IP address. If you can determine that the attack is coming from a specific IP address, block access from that IP address. Set an appropriate password that is not the default one.Measures to pass on the damage through insurance are effective. Measures to pass on the damage through insurance are effective.
10	Cyber attack	Low	High	Risk Transference	In addition to the basic security measures, it is necessary to improve the attention of users. In addition to the basic security measures, it is effective to improve the user's attention, and take measures to pass the cost on through insurance, etc.
11	Vulnerability of IoT devices	Low	High	Risk Transference	Check access logs and communication logs, etc., and if it can be determined that the attack is being conducted from a specific IP address, prevent access from that IP address. If you can determine that the attack is coming from a specific IP address, block access from that IP address. Keep the OS and firmware up to date. Measures to pass on the damage through insurance are effective.
12	Supply chain vulnerabilities	Low	High	Risk Transference	Sharing of the latest attack information among companies in the supply chain. Sharing of the latest attack information among companies in the supply chain, cooperation, and collaboration in clarifying and sharing management measures for critical information. Implementation of unified security measures. Measures to be passed on through insurance, etc. are effective.
13	SNS	Low	High	Risk Transference	It is also important to educate people on how to handle information assets when using social networking services and to develop their own platforms. Measures to shift the risk through insurance are effective.
14	Improper internal behavior	Low	High	Risk Transference	Provide regular security governance and security policy training to employees.
15	Burnout	Low	High	Risk Transference	Drastic elimination of the environment that caused the burnout.
16	Slip	Low	High	Risk Transference	Identification of error-prone tasks and improvement of the work flow to prevent recurrence. Addition of alerting and confirmation processes. Sharing examples of near misses in the organization.
17	Mistake	Low	High	Risk Transference	Identification of error-prone tasks and improvement of the work flow to prevent recurrence. Sharing of near miss cases in the organization. Educate the employees so they can gain knowledge and motivation for the work.
18	Lapse	Low	High	Risk Transference	Identification of error-prone tasks and improvement of the work flow to prevent recurrence. Creating an environment where feedback can be obtained. Sharing examples of near misses in the organization.
19	Negligence	Low	High	Risk Transference	The security measures for products and systems are based on the design concept of security by design. Security measures for products and systems should be comprehensive from the design stage, including measures after operation. Security measures for products and systems should be considered from the design stage to be comprehensive, including post-operation measures.
20	GDPR	Low	High	Risk Transference	Check for access from within the EU, and ensure that products and services destined for the EU comply with the GDPR. Data vendors should make sure that the sources of their data are GDPR-compliant. Companies that sell data should be GDPR-compliant, etc.
21	Responsibility decomposition point	Low	High	Risk Transference	Both contractors and subcontractors in the IT supply chain should review the templates of contract-related documents and establish guidelines and risk assessments. Development of guidelines and risk assessment by the contractor and the subcontractor are cited as countermeasures. Measures to pass the risk on through insurance, etc. are effective.
22	Illegal mining of virtual currency	Low	High	Risk Transference	In addition to basic security measures, install security software and keep the definition files up-to-date. Insurance is an effective measure.
23	AI	Low	High	Risk Transference	Promote discussion and consensus building between the public and private sectors on measures to prevent tampering with training data, the scope of responsibility for AI use in practical operations, legal systems, and collaboration between users and AI.

3.3 Risk Evaluation of Silent Cyber Risks

In this section, we evaluate the effectiveness of the countermeasures proposed in Table 5 based on their quantification by risk values. Specifically, we utilize a risk formula commonly used in the ISMS field [19].

3.3.1 Ordinary Risk Value Formula

Each risk value can be quantified by Eq. (1), which is commonly used in the field of ISMS [13].

Risk value = value of asset × value of threat × value of vulnerability (1)

Here, in general, all elements on the right-hand side of Eq. (1) are very difficult to calculate. We use the following approximation to simplify these elements [20].

3.3.2 Approximate Risk Value Formula for Risk Evaluation

(1) Approximation of Asset Values and Threats
To simplify the quantification of risk countermeasures, the asset value and threat in Eq. (1) are approximated to the impact and frequency of occurrence in the risk matrix, as shown in Fig. 6 [20]. Specifically, we approximate the asset value as the impact and define the risk value between 5 (high) and 1 (low), referring to the literature [19]. In the same way, we approximate the threat as the frequency of occurrence and define the risk value between 3 (high) and 1 (low) [14].

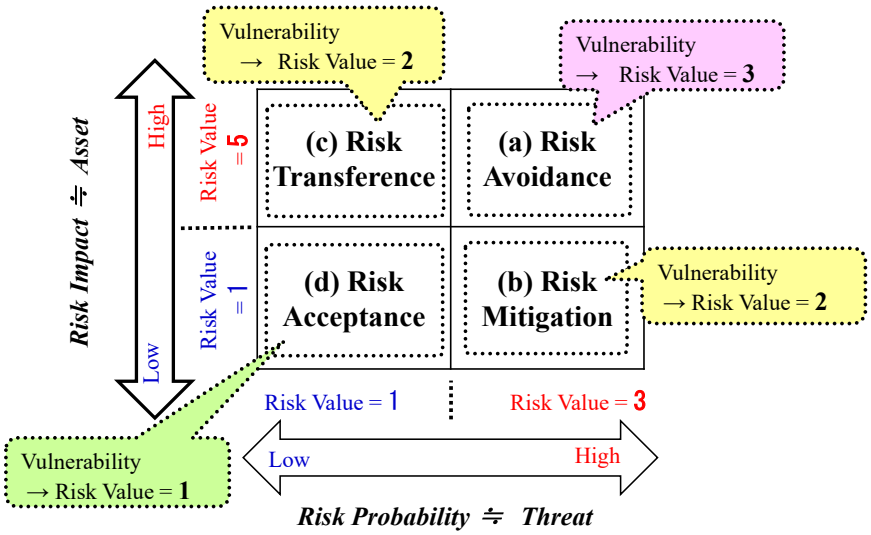


Figure 6: Quantifying the risk matrix with approximation.

(2) Approximation of Value of Vulnerability
Next, we approximate the vulnerability by referring to the literature [19] and using the risk matrix [20]. We use three levels of evaluation and approximate Risk Avoidance as 3 (high), Risk Transference and Risk Mitigation as 2 (medium), and Risk Acceptance as 1 (low).

(3) Approximate Risk Value Formula
By approximating (1) and (2), Eq. (1) becomes Eq. (2).

Risk value = value of risk impact × value of risk probability × value of vulnerability (2)

3.3.3 Calculation of Risk Value Based on Eq. (2)

Here, we evaluate the risk countermeasures by using Eq. (2) for calculating the risk values. First, the risk values before risk countermeasures are shown in Table 6. Next, the risk values after risk countermeasures have been applied are shown in Table 7.

(1) Calculation of Risk Value Before Countermeasures
First, the results of calculating the risk values before risk countermeasures are shown in Table 6.

(2) Calculation of Risk Value After Countermeasures
Next, the results of the calculation of the risk values after the risk countermeasures have been applied are shown in Table 7. Here, the vulnerability is approximated to be 1 (low) after the risk countermeasure implementation.

Table 6: Risk assessment before countermeasures.

No.	Risk Factors	Risk Probability（P）	Risk Impact（I）	Vulnerability（V）	Risk Value
1	Earthquake	1	5	2	10
2	Tsunami	1	5	2	10
3	Typhoon	1	5	2	10
4	Volcanic activity	1	5	2	10
5	Pandemic	1	5	2	10
6	War and terrorism	1	5	2	10
7	Cyberterrorism	1	5	2	10
8	Cyber attack	1	5	2	10
9	Vulnerability of IoT devices	1	5	2	10
10	Cyber attack	1	5	2	10
11	Vulnerability of IoT devices	1	5	2	10
12	Supply chain vulnerabilities	1	5	2	10
13	SNS	1	5	2	10
14	Improper internal behavior	1	5	2	10
15	Burnout	1	5	2	10
16	Slip	1	5	2	10
17	Mistake	1	5	2	10
18	Lapse	1	5	2	10
19	Negligence	1	5	2	10
20	GDPR	1	5	2	10
21	Responsibility decomposition point	1	5	2	10
22	Illegal mining of virtual currency	1	5	2	10
23	AI	1	5	2	10

Table 7: Risk assessment after countermeasures.

No.	Risk Factors	Risk Probability（P）	Risk Impact（I）	Vulnerability（V）	Risk Value
1	Earthquake	1	5	1	5
2	Tsunami	1	5	1	5
3	Typhoon	1	5	1	5
4	Volcanic activity	1	5	1	5
5	Pandemic	1	5	1	5
6	War and terrorism	1	5	1	5
7	Cyberterrorism	1	5	1	5
8	Cyber attack	1	5	1	5
9	Vulnerability of IoT devices	1	5	1	5
10	Cyber attack	1	5	1	5
11	Vulnerability of IoT devices	1	5	1	5
12	Supply chain vulnerabilities	1	5	1	5
13	SNS	1	5	1	5
14	Improper internal behavior	1	5	1	5
15	Burnout	1	5	1	5
16	Slip	1	5	1	5
17	Mistake	1	5	1	5
18	Lapse	1	5	1	5
19	Negligence	1	5	1	5
20	GDPR	1	5	1	5
21	Responsibility decomposition point	1	5	1	5
22	Illegal mining of virtual currency	1	5	1	5
23	AI	1	5	1	5

3.3.4 Evaluation Results of Risk Value Formula

Table 8 shows the changes in risk values before and after the risk countermeasures based on the results of Tables 6 and 7.

Table 8: Risk values before and after countermeasures.

	Total risk value = Σ(Value of risk impact × value of risk probability × value of vulnerability)
Before risk countermeasures (1)	230
After risk countermeasures (2)	115
Risk value reduction rate = ((1)-(2))/ (1)	0.5

From Table 8, we can see that the risk value was reduced by 50% when the risk countermeasure was applied to the silent cyber risk compared to that before the risk countermeasure. Although

this is a relative index of risk value, it can be considered to function as a reference when applying specific risk countermeasures.

4 Considerations: Portfolio Management

In this section, we discuss the results of the silent cyber risk assessment from a practical perspective. In general, silent cyber risks can have a fatal impact on organizational activities, so it is important to take countermeasures in advance. However, from a practical point of view, it is necessary to consider the priority of the countermeasures. In this section, we apply portfolio management based on the return on investment to the risk countermeasures for silent cyber risks proposed in Section 3. Specifically, we evaluate the countermeasures for silent cyber risk based on portfolio management as shown below.

4.1 Application of Portfolio Management

We applied the CSIRT system here as a general system of countermeasures for the portfolio of security countermeasures in an organization. In CSIRT, three elements are considered important as security countermeasures: security pre-measures (Proactive Service), security post-measures (Reactive Service), and security quality countermeasures (Security Quality Management Service). Therefore, in this section, a portfolio based on these three elements for the security countermeasures proposed in Section 3 is performed as a portfolio management.

4.2 Alteration Risk

In this subsection, we evaluate the risk of alteration. As shown in Table 9, the alteration risk is caused by natural disasters and human factors. Since the risks here are expected to cause enormous damage, such as the destruction of an organization, it is essential to take countermeasures in advance, such as BCP/DR countermeasures. Preventing sudden and complex occurrences in advance is very effective and has the highest priority. It is also necessary to reduce the risk of security quality by improving the operational quality of the advance countermeasures.

The meanings of the symbols in the tables below are as follows.

◎: Very high priority
○: High priority
△: Medium priority
Blank: Low priority

Table 9: Portfolio of risk countermeasures for alteration risk.

No	Risk Factors	Outline of countermeasures	Pre	Post	Quality
1	Earthquake	Take anti-vibration measures to reduce the impact of earthquakes, and store frequent backups in the cloud or other cyberspace. Measures such as insurance are effective.	◎		○
2	Tsunami	Avoid locations that may be submerged in water, such as offices on two or more floors and waterproofing of hardware devices. Avoid locations where there is a risk of submersion. Also, back up frequently. Store data in cyberspace, such as in the cloud. Measures such as insurance are effective.	◎		○
3	Typhoon	Consider installing an emergency power supply and make frequent backups in the cloud or other cyberspace. Store the data in cyberspace. Measures to pass on the losses through insurance are effective.	◎		○
4	Volcanic activity	Use of dust-proof hardware and frequent backups. Store in cyberspace, such as in the cloud. Insurance is an effective measure.	◎		○
5	Pandemic	Formulation of security policies for activities outside the office, and implementation of security education, etc. Measures to pass the cost on through insurance, etc. are effective.	◎		○
6	War and terrorism	Store frequent backups in the cloud or other cyberspace. Measures to pass on the damage through insurance are effective.	◎		○
8	Cyberterrorism	Acquisition of backups to prevent ransomware. It is also important to prepare a response flow for recovery, conduct training, and implement recovery tests. Measures to pass the cost on through insurance are effective.	◎		○

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service
◎: Very high priority, ○: High priority, △: Medium priority, Blank: Low priority

4.3 Combination Risk (Cyber × Physical)

In this subsection, we evaluate the combination risk (cyber × physical). As shown in Table 10, the combined risk (cyber × physical) is characterized by the fact that it is caused by an external attack. As shown in Table 10, the combined risk (cyber × physical) is also characterized by the fact that it is caused by an external attack, and therefore, the post-incident response is expected to result in fatal damage. Therefore, in the case of combined risk (cyber × physical), it is effective to control the occurrence and take countermeasures in advance. In addition, countermeasures that continue to ensure the quality of operations should be given the highest priority.

Table 10: Portfolio of risk countermeasures for combination risk (cyber × physical).

No	Risk Factors	Outline of countermeasures	Pre	Post	Quality
7	Cyber attack	In addition to basic security measures, improve the attention of users. Measures to pass the cost on through insurance, etc. are effective.	○		◎
9	Vulnerability of IoT devices	Check access logs and communication logs, etc., and if it can be determined that the attack is being conducted from a specific IP address, prevent access from that IP address. If you can determine that the attack is coming from a specific IP address, block access from that IP address. Set an appropriate password that is not the default one. Measures to pass on the damage through insurance are effective.	○		◎
10	Cyber attack	In addition to the basic security measures, it is necessary to improve the attention of users. In addition to the basic security measures, it is effective to improve the user's attention, and take measures to pass the cost on through insurance, etc.	○		◎
11	Vulnerability of IoT devices	Check access logs and communication logs, etc., and if it can be determined that the attack is being conducted from a specific IP address, prevent access from that IP address. If you can determine that the attack is coming from a specific IP address, block access from that IP address. Keep the OS and firmware up to date. Measures to pass on the damage through insurance are effective.	○	△	◎
12	Supply chain vulnerabilities	Sharing of the latest attack information among companies in the supply chain. Sharing of the latest attack information among companies in the supply chain, cooperation, and collaboration in clarifying and sharing management measures for critical information. Implementation of unified security measures. Measures to be passed on through insurance, etc. are effective.	○		◎
13	SNS	It is also important to educate people on how to handle information assets when using social networking services and to develop their own platforms. Measures to shift the risk through insurance are effective.	○		

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service
◎: Very high priority, ○: High priority, △: Medium priority, Blank: Low priority

4.4 Combination Risk (Cyber × Psychology)

In this subsection, we evaluate the combination risk (cyber × psychology). As shown in Table 11, the combination risk (cyber × psychology) is characterized by the fact that it is caused by an attack from the inside. The impact of risk incidents originating from the inside is enormous, and the conditions for their occurrence tend to depend on the external environment, such as the triangle of injustice. Therefore, it is effective to control the occurrence of risk incidents and to take countermeasures in advance. In addition, it is very important to prevent these incidents from becoming a skeleton, and therefore, countermeasures to continue to ensure the quality of operations are of the highest priority.

Table 11: Portfolio of risk countermeasures for combination risk (cyber × psychology).

No	Risk Factors	Outline of countermeasures	Pre	Post	Quality
14	Improper internal behavior	Provide regular security governance and security policy training to employees.	○		◎
15	Burnout	Drastic elimination of the environment that caused the burnout.	○		◎
16	Slip	Identification of error-prone tasks and improvement of the work flow to prevent recurrence. Addition of alerting and confirmation processes. Sharing examples of near misses in the organization.	○		◎
17	Mistake	Identification of error-prone tasks and improvement of the work flow to prevent recurrence. Sharing of near miss cases in the organization. Educate the employees so they can gain knowledge and motivation for the work.	○		◎
18	Lapse	Identification of error-prone tasks and improvement of the work flow to prevent recurrence. Creating an environment where feedback can be obtained. Sharing examples of near misses in the organization.	○		◎
19	Negligence	The security measures for products and systems are based on the design concept of security by design. Security measures for products and systems should be comprehensive from the design stage, including measures after operation. Security measures for products and systems should be considered from the design stage to be comprehensive, including post-operation measures.	○		

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service
◎: Very high priority, ○: High priority, △: Medium priority, Blank: Low priority

4.5 Combination Risk (Cyber × Environment)

In this subsection, we evaluate the combination risk (cyber × environment). As shown in Table 12, for the combination risk (cyber × environment), the priority is to respond promptly after the fact and to ensure compliance in operations, as shown in GDPR. In addition, it is relatively effective to respond in advance. Clarifying the position in the environment in advance makes it easier to respond when changes occur and to recognize exposures.

Table 12: Portfolio of risk countermeasures for combination risk (cyber × environment).

No	Risk Factors	Outline of countermeasures	Pre	Post	Quality
20	GDPR	Check for access from within the EU, and ensure that products and services destined for the EU comply with the GDPR. Data vendors should make sure that the sources of their data are GDPR-compliant. Companies that sell data should be GDPR-compliant, etc.		◎	○
21	Responsibility decomposition point	Both contractors and subcontractors in the IT supply chain should review the templates of contract-related documents and establish guidelines and risk assessments. Development of guidelines and risk assessment by the contractor and the subcontractor are cited as countermeasures. Measures to pass the risk on through insurance, etc. are effective.	△	◎	○
22	Illegal mining of virtual currency	In addition to basic security measures, install security software and keep the definition files up-to-date. Insurance is an effective measure.	△	◎	○
23	AI	Promote discussion and consensus building between the public and private sectors on measures to prevent tampering with training data, the scope of responsibility for AI use in practical operations, legal systems, and collaboration between users and AI.		◎	○

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service
◎: Very high priority, ○: High priority, △: Medium priority, Blank: Low priority

4.6 Summary of Portfolio of Risk Countermeasures for Silent Cyber Risks

In countermeasures against silent cyber risks, the priority is to take proactive countermeasures. However, the introduction of countermeasures in advance may be more costly and excessive compared to the application of countermeasures after the fact. Therefore, as discussed in subsections 4.2 to 4.5, it is effective to take appropriate proactive countermeasures and then to ensure and enhance the quality of relatively low-cost operational countermeasures to deal with silent cyber risks.

5 Conclusion and Future Work

In this paper, we clarified through a literature review that silent cyber risk has the characteristics of both emerging and systemic risks. On the basis of our findings, we defined “Alteration risk” and “Combination risk” as the risks of transitioning to different states, and then newly defined

and modeled silent cyber risk. Especially, for "Combination risk", we defined the areas connected to cyberspace as physical, psychological, and environmental, and then comprehensively extracted the silent cyber risks. A total of 23 risk factors were extracted and analyzed, and we identified the most effective risk countermeasures for "Alteration risk" (namely, passing on the risk through insurance and other countermeasures) and for "Combination risk" (namely, reducing the impact of the risk factors themselves). We also conducted a risk value assessment to evaluate the proposed countermeasures and found that they could reduce the risk by approximately 50%, which demonstrates the effectiveness of the proposed countermeasures against silent cyber risk in organizations.

In Section 4, the results of the silent cyber risk assessment were discussed from an operational point of view. In addition, portfolio management was applied to the risk countermeasures for the silent cyber risks proposed in Section 3 based on the return on investment. The results showed that the priority of proactive countermeasures tended to be high in the case of silent cyber risks. However, the introduction of proactive countermeasures may be costlier than security post-measures and may lead to excessive countermeasures. In conclusion, we clarified that to effectively prevent silent cyber risks, it is effective to ensure and improve the quality of relatively low-cost operational countermeasures after taking appropriate proactive measures.

Our future work will include the development of a detailed visualization model of silent cyber risk through scoring and other methods. We also intend to investigate the "unknown-unknowns" risk.

Acknowledgement

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

References

[1] Ministry of Internal Affairs and Communications, 2020 White Paper on Information and Communication, 2020, (Japanese Edition).

[2] Ministry of Economy, Trade and Industry, Cyber-physical security countermeasure framework, 2019, https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf, (Japanese Edition).

[3] N. Kin, Trends in Silent Cyber Risk: Focusing on the United States and the United Kingdom- P&C Insurance Report No. 126, 2019, (Japanese Edition).

[4] T. Yoshizawa, How should insurers deal with emerging risks these days, The Insurance Society of Japan and The Risk Research Society of Japan Joint Special Session, 2017, (Japanese Edition).

[5] Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK GUIDE) Sixth Edition, Project Management Institute, 2017.

[6] IEC 31010:2019 Risk management — Risk assessment techniques.

[7] H. Nagata, Systemic Risk and Financial Vulnerability, Fukuoka University Business Series

57 (3-4), end of volume 1-5,2013, (Japanese Edition).

[8] M. Ando, Nikkei Cross Tech / Nikkei NETWORK, The average annual damage is 148 million yen, and there are two effective measures against cyber attacks., 2020, (Japanese Edition).

[9] National Institute of Information and Communications Technology, Release of NICTER Observation Report 2020, 2020, (Japanese Edition).

[10] ISO 31000: 2018 Risk management — Guidelines.

[11] Tokio Marine & Nichido Fire Insurance Co., Presentation materials for the second meeting of the Information Disclosure Subcommittee of the Cyber Security Task Force, 2018, (Japanese Edition).

[12] R. Mishina, et al., Risk Management of Silent Cyber Risks in Consideration of Emerging Risks, 2021 10th International Congress on Advanced Applied Informatics (IIAI-AAI), pp.710-716, 2021

[13] M. Baezner, et al., Stuxnet. 2017. Available online: https://css.ethz.ch/ (accessed on 17 November 2023).

[14] R. Mishina, et al., A Visualization Model for Silent Cyber Risks Contained in Emerging Risks, 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE), pp.575-576, 2021

[15] R. Mishina, et al., An Extended Visualization Model for Silent Cyber Risks Considering Non-cyber Aspects, 2022 IEEE 11th Global Conference on Consumer Electronics (GCCE), pp.277-278, 2022

[16] S. Tanimoto, et al., Risk Countermeasures Based on Five Whys Analysis Considering Offensive Security, 2023 IEEE 12th Global Conference on Consumer Electronics (GCCE), pp.643 - 645, 2023

[17] G. Ahn, et al., Malicious File Detection Method using Machine Learning and Interworking with MITRE ATT&CK Framework. Appl. Sci. 2022, 12, 10761

[18] R. Abdullahi et al., Fraud prevention initiatives in the Nigerian public sector: understanding the relationship of fraud incidences and the elements of fraud triangle theory, Journal of Financial Crime, https://doi.org/10.1108/JFC-02-2015-000

[19] H. Sato, et al., Information Security Infrastructure, Kyoritsu Shuppan Co., Ltd., 2010, (Japanese Edition)

[20] 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.