Cybersecurity Management Guidelines

Ver 1.1

Ministry of Economy, Trade and Industry (METI)

Independent Administrative Agency Information-technology

Promotion Agency (IPA)

Contents

Outline of the cybersecurity management guidelines

1. Cybersecurity is a management issue

- **Making the best use of IT has become indispensable for improving corporate profitability** in a variety of business scenes, for example, when personal information of customers are collected and utilized, technical intelligence as a trade secret is applied, or plants are automatically regulated.
- In the meantime, **cyber-attacks** aimed at businesses **present an unavoidable risk**. They could cause a serious issue to companies, **some of which even have actually lost more than half of their net profits due to cyber-attacks**. **As a preventative measure, investment in security** is crucial. What this means is that management decision is required from the corporate strategic viewpoint for how much **IT investment** should be made, and at the same time, how much **security investment** should be made for maintaining part of corporate value, that is, ensuring business continuity and improving defense capabilities against cyber-attacks.
- As well, **in cases where damage has also been caused to the society** through leakage of personal information or sensitive technologies for security, or suspension of infrastructural services due to cyber-attacks, **corporate management will be severely questioned by the public as to whether their approach for risk management was adequate or not**.
- These guidelines are aimed at the management of companies which have a dedicated division for information system and are utilizing IT, and include, from the viewpoint of protecting companies from cyber-attacks, **2. "3 Principles" which the management need to recognize**, and **3. "10 Important Items" which the management should direct their executives in charge to observe.**

2. "3 Principles" which the management need to recognize

(1) Now, the instances of companies providing IT services and utilizing IT for the purpose of business development or enhancement of their productivity are on the rise. Therefore, cyber-attacks have become almost inevitable, and investment in security is vital as a part of any sound business strategy, and therefore management is responsible for ensuring this. For this reason, **the management need to take the leadership in promoting measures** regarding how much risk the company is willing to take of cyber-attacks and how much investment should be made in security. **Otherwise risk which could hugely affect their company would be overlooked.**

(2) Great risk factors include not only problems in the company's subsidiaries but also leakage of information provided outside the company such as outsourcing contractors for production due to cyber-attacks. For this reason, **comprehensive security measures are necessary covering the company itself, its group companies, and business partners of its supply chain.**

(3) In order to improve trust of customers and stockholders as well as mitigate the distrust in case of having faced a cyber-attack, companies **need to communicate appropriately with relevant parties by, for example, disclosing information on security measures at ordinary times**.

3. "10 Important Items" which the management should direct their executives in charge to observe

Direction 1: **Announce a security policy** for cybersecurity risk management in and outside the organization.

Direction 2: **Build an appropriate management structure** made of the corporate management, security managers, and CISO (Chief Information Security Officer: director in charge of managing information security in the company) as a mediator in order to ensure that measures based on the policy are properly taken.

Direction 3: **Specify assets to be protected**, **discover all the security risk**, and **develop a plan for risk management** based on the management strategy.

Direction 4: **Implement PDCA** in order to ensure that the plan is surely carried out and that improvement will be made. As well, the implementation status needs to be **reported to the management regularly by CISO** and **appropriately disclosed to improve the trust** of stakeholders.

Direction 5: Make sure that **group companies and business partners of the company's supply chain** take **security measures including implementation of PDCA** the way the company does.

Direction 6: In order to prepare for **stable execution of cybersecurity measures** including PDCA implementation, **examine resource management including securing necessary budget and developing personnel**.

Direction 7: **Appropriately divide task** of IT system operation from the viewpoint of the company's technical capabilities and efficiency **into that which the organization itself should take care of and that which outsourcing organizations should handle.** As well, in case of outsourcing, make sure that **cybersecurity against attacks on the outsourcing contractors is ensured**.

Direction 8: **Participate in information sharing activities and update the company's measures according to the latest attacks** because hackers keep strengthening their offensive capabilities. As well, contribute as much as possible to **prevention of similar damage from being broadly given to the society** by **providing the information on attacks which the company came under to public information sharing activities**.

Direction 9: In case of facing a cyber-attack, **prevent further damage by taking prompt initial actions.** To this end, **establish CSIRT (Computer Security Incident Response Team)** and, at the same time, develop an **initial action manual**. As well, implement **regular training**.

Direction 10: To provide against a cyber-attack, **organize information on who needs to be notified and what needs to be disclosed after discovering damage**, and **make sure that the management can give a necessary account of the situation** both to the company and public **without delay**.

1. Introduction

1.1. Background and positioning of Cybersecurity Management Guidelines

Recent years have seen increases in cyber-attacks by which attackers try to steal personal and technological information owned by companies or other organizations, or to shut down their systems, and about 40% of companies have experienced cyber-attacks (see Fig. 1). Targeting methods have become increasingly sophisticated as they focus on certain organizations using target-oriented attack techniques. It's likely that most victim companies are not aware of being damaged by cyber-attacks due to the fact that about 70% of reported incidents on cyber-attacks are reported by people outside the company (see Fig. 2). Furthermore, cyber-attacks have begun to impact real world assets as systems and devices owned by companies including control systems for their infrastructure, manufacturing plants etc. are connected to external networks.

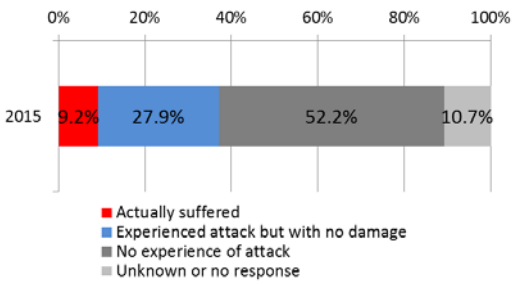
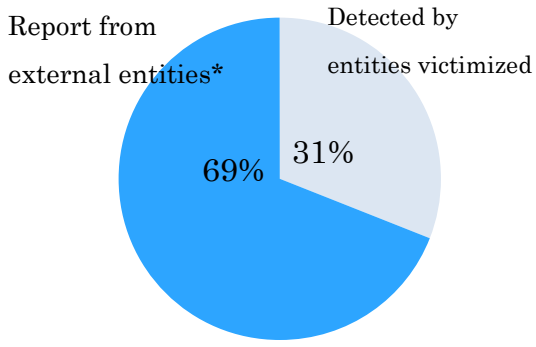


Fig.1 Ratio of companies which suffered damage by cyber-attacks(excluding computer virus)[1]



*partners, customers, investigating authorities etc.

Fig.2 How security breach was detected.[2]

Thus we have witnessed increasingly threat of cyber-attacks directed to companies although we cannot be assured if many companies are committed to measures to address them. One of the reasons might be that the management have insufficient capability as leaders to deal with cybersecurity measures. Our country indicates less management involved in pursuing cybersecurity measures than those in overseas countries (see Fig. 3). Additionally, taking into account that most overseas companies regard the issue of cyber-attacks as an important agenda for discussion among board members, this

[1] Prepared by the Ministry of Economy, Trade and Industry based on the "Report on the investigation into CISO and CSIRT in companies 2016" by the Information Technology Promotion Agency (Independent Administrative Institution)

[2] Prepared by Ministry of Economy, Trade and Industry based on "M-trends2015: Perspective of security measures forefront" by FireEye Inc.

awareness is lagging in Japan, though it is spreading to a certain extent (see Fig. 4).

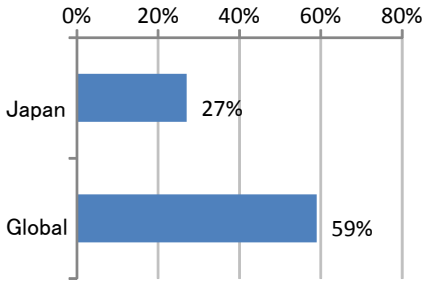


Fig.3 Companies whose management actively drive security measures.[3]

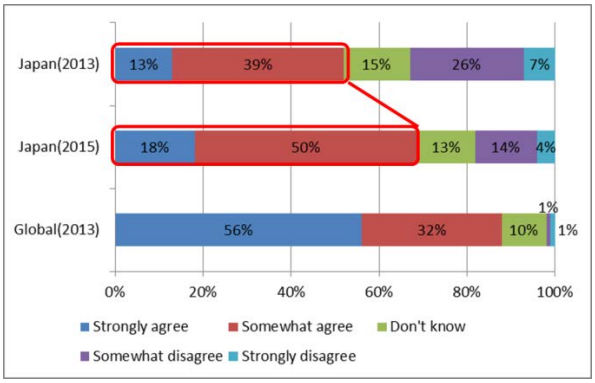


Fig.4 Level in organization for discussion on cyber-attack response.[4]

IT investment has actively been implemented as an important element in furthering corporate competitiveness. At this point it is one of management's roles to be aware of the strategic importance and role of confidential information, including trade secrets and of information systems which are necessary for company's business and to make appropriate decisions in addressing the risk of cyber-attacks. On the other hand, though the investment in measures to ensure cybersecurity is essential, the return on investment seems difficult to quantify. Therefore, management is required to show leadership in actively accelerating these measures. This vagueness in predicting return might cause companies to be less prepared for risk management and to be forestalled in addressing risk even if crisis occurs to them, and eventually to experience situation that rocks company management before they know it.

Against this backdrop the cybersecurity management guidelines were developed to collectively publish principles that the management should follow and tasks that company executives should perform as leaders. Technically these guidelines include contents on how to drive organization and measures relating to security risk under the leadership of the management as well as how the disclosure of information should be handled to the public or stakeholders. These guidelines are primarily intended for companies' management who commit themselves to strengthen cybersecurity measures as leaders.

These guidelines are also targeted at major/medium/small businesses (excluding tiny business) which supply products, systems or services related to IT and those for which

[3] Prepared by Ministry of Economy, Trade and Industry based on "2014 Global State of Information Security Survey" by PricewaterhouseCoopers Co., Ltd.

[4] Prepared by Ministry of Economy, Trade and Industry based on "Security Survey 2013", "Security Survery 2016" by KMPG Japan

the utilization of IT is vital from the viewpoint of business strategy. However, it should be noted that these guidelines do not necessarily provide comprehensive, individual measures for cybersecurity for every size of business or business model.

These guidelines were put together based on the result of an exploratory session titled "Study on cybersecurity risk and corporate management" jointly sponsored by the Ministry of Economy, Trade and Industry and the Information Technology Promotion Agency (Independent Administrative Institution) (hereafter "IPA"). Furthermore, the National center of Incident readiness and Strategy for Cybersecurity (NISC) published "Approaches to cybersecurity for corporate management"[5], a document that introduces a fundamental approach to cybersecurity and how to cope with the issue from different points of view. This document has been released to promote voluntary corporate management efforts based on the idea that cybersecurity is a necessary "investment" in more active management in the current changing environment of global competition. It is hoped that the aforementioned document will be used together with these Guidelines as it is the document from which the basic idea of these Guidelines derived.

[5] This document can be downloaded at website of NISC (http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf).

1.2. Structure and use of the Guidelines

The structure of the guidelines is as follows.

Top summary is intended for the management. Sections of Chapter 2, Chapter 3, and appendix A serve for officers responsible for cybersecurity measures or relevant officers (hereinafter "CISO"). Other appendix is information for personnel in charge of security task.

Cybersecurity Management Guidelines
1. Introduction
2. Three principles of cybersecurity management
3. Ten important items of cybersecurity management (Appendix)
A) Check sheet of cybersecurity management
B) Expected technical measures
C) In relation to International Standard ISO/IEC 27001 and 27002
D) Definition of terms

The management are required to review at least the overview, and subsequently to give directions on ten important items to CISO.

CISO is required to drive security task based on the instruction from the management by giving more detailed directions to personnel in charge of security while referring to "examples of measures" described in explanatory pages regarding the important ten items. Besides these tasks they need to review whether or not these ten important items are formally and virtually followed, and to revert it to the management. Appendix A provides the check sheet to ensure their efforts of reviewing.

Besides this reviewing efforts, from perspective of technical element Appendix B provides items expected to be followed by personnel in charge of security based on instructions from CISO. It is expected that these Appendices will serve as reference for discussion or consultation between CISO and personnel in charge of security.

Appendix C as reference indicates the relationship with International Standard ISO/IEC 27001 and 27002. This will support efforts of confirmation of measures to be taken or report to the management regarding status or review of each item.

Appendix D provides glossary used in the guidelines and helps the management to produce materials.

With respect to risk regarding leakage of information committed internally, more effective actions become possible though reference to "Guidelines for the Prevention of Internal Improprieties in Organizations" by IPA where necessary.[6]

[6] This information can be downloaded at website (https://www.ipa.go.jp/files/000044615.pdf).

2. Three principles of cybersecurity management

It is necessary for the management to take note of the following three principles to proceed with countermeasures.

(1) The management are required to drive cybersecurity risk measures considering any possible risk while in proceeding with the utilization of IT.

(Explanation)

- Now, the instances of companies providing IT services and utilizing IT for the purpose of business development or enhancement of their productivity are on the rise. Therefore, cyber-attacks have become almost inevitable, and investment in security is vital as a part of any sound business strategy, and therefore management is responsible for ensuring this.
- In cases where cyber-attacks compromise business continuity or give rise to leakage of information, whether or not companies are capable of swiftly and appropriately responding to it determines life or death.
- For this reason it is vital that management should utilize their leadership and available resources to take necessary countermeasures against cybersecurity risks, while at the same time announcing response policy to company's staff and to people outside the company and regard cybersecurity risk as an important factor in risk management. Additionally, responding to the changing cybersecurity risks and incorporating past lessons learned into corporate policy to ensure that incidents are not repeated must be added to this effort.

(2) Comprehensive security measures are necessary covering the company itself, its group companies, business partners of its supply chain and IT system control outsourcing companies.

(Explanation)

- In the case that there are cyber-attacks on business partners or outsourcing companies of IT system , the concern arises that information provided by the company might be compromised.
- Comprehensive security measures are necessary covering the company itself, its group companies, business partners of its supply chain and outsourcing companies of IT system control.

(3) Companies need to communicate appropriately with relevant parties by, for example, disclosing information on security measures or response on regular basis or in times of emergency.

(Explanation)

- It is necessary to strengthen trust with clients or relevant parties by sharing information on response for cybersecurity risk involved in the business.
- Even in the case of cyber-attacks causing some damage, the constant communication with relevant parties on regular basis will help to subdue distrust from them and also to facilitate accountability for such damage. Moreover sharing information on cyber-attacks (incident information) are expected to serve to prevent similar damage from happening to other entities.
- Thus companies need to continue communication with relevant parties or partners to let them know that cybersecurity measures are in place for the applicable business.

3. Ten important items of cybersecurity management

The management are required to steadily drive cybersecurity measures by giving CISO directions on the following ten important items.

1. **Display leadership and build a structure or process.**
   (1) Recognize a cybersecurity risk and develop company-wide measures.
   (2) Build a structure or process for a cybersecurity risk management.

2. **Determine framework for a cybersecurity risk management.**
   (3) Determine goals and develop plans based on perception of a cybersecurity risk and security level that should be attained.
   (4) Publish cybersecurity measures framework (PDCA) and their actions.
   (5) Make sure as to how group companies and business partners of the company's supply chain take security measures.

3. **Develop proactive measures to prevent cyber-attacks.**
   (6) Secure resource (budget, manpower etc.) to execute cybersecurity measures.
   (7) Identify the scope of outsourcing with IT system control and ensure cybersecurity in the applicable outsourcing companies.
   (8) Collect and utilize information on cyber-attacks through participation in information sharing activities, and develop environment to utilize such information

4. **Prepare in case of cyber-attacks occurrence**
   (9) Develop emergency response system (emergency contacts and initial action manual, CSIRT - Computer Security Incident Response Team), Execute regular and hands-on drill.
   (10)Collect information regarding contacts, and gather information to be disclosed, and prepare materials for the management's accountability.

3.1. Display leadership and build a structure or process

(1) Recognize a cybersecurity risk and develop company-wide measures.

Is a cybersecurity risk regarded as one important element among a variety of management risk facing them, and are company-wide measures (security policy) in place?

Scenario in case of no action for security

*By publishing cybersecurity measures the management can let all personnel in an organization know about their idea regarding measures. Without this act of publishing or announcing them, what personnel in an organization will perform for security tends to be inconsistent with an organizational policy.

*This act of publishing or announcing them will heighten trust of shareholders, customers and business partners, leading to the increase in value of the brand. However without such act, there is no enhancing trust.

Example of recommended actions

*Develop security policy incorporating cybersecurity risk management while aligning it with the management policy of a company so that the management can publish company-wide measures.

(2) Build a structure or process for cybersecurity risk management.

Has s structure or process for cybersecurity risk management been in place, which acts as bridge between the management and personnel in charge of cybersecurity in driving security measures? Has responsibility of each relevant person been defined? Furthermore has such responsibility been consistent with other risk management divisions such as crime prevention?

Scenario in case of no action for security

*Without a structure or process for a cybersecurity risk management, to grasp the status of a cybersecurity risk becomes impossible.

*If a designated CISO were not granted authority, it is impossible to become aware of a cybersecurity risk from perspective of technology and business strategy. If management-level authority is not given to CISO where they need to determine whether or not suspend cyber-attacked system which might compromise business continuity, they will not be able to cope with such attack. This absence of authority also triggers the issues of vague and unclear responsibility,

*No aligning cybersecurity risk response system with other response systems within the same organization will cause redundancy of similar activities, and result in no sharing of relevant information, which is inefficient.

*In case of any sort of incident occurrence, an organization without established structure or process will not be able to take proper steps including the grasp of damage situation, examination of cause, the way damage should be reduced and prevention of incident recurrence.

Example of recommended actions

*Establish a committee on management risk and allow responsible personnel of a cybersecurity risk to become a member of such committee.

*Designate CISO according to the policy on company-wide measures (or security policy), and establish a structure or process for a cybersecurity risk management within an organization.

*Consider if CISO can be granted the management-level authority to allow them to attend a meeting of the board of directors to grasp an organizational business strategy and to enable them to stop various systems in case of emergency.

*Directors and auditors should audit such structure or process for a cybersecurity risk management if it is properly established and works accordingly.

3.2. Determine the framework for a cybersecurity risk management.

(3) Determine goals and develop plans based on perception of a cybersecurity risk and security level that should be attained.

Do you give direction to grasp the status of a cybersecurity risk such as internal network while making them identify assets to be protected from perspective of business strategy to address threat of cyber-attacks? Do you provide direction in determining goals and developing plans for countermeasures according to risk such as multi-layer protective systems composed of different cybersecurity measures, e.g. encryption, segregation of networks etc.? Do you give direction to consider transfer of risk by using cyber insurance or entrusting assets to be protected with professional service providers and then to identify outstanding risk?

Scenario in case of no action for security

*All companies and organizations are faced with any sort of cybersecurity risk. On the other hand risk varies depending on assets to be protected (personal information, technical intelligence etc.) or current network environment within companies or organizations

*Without proper risk management measures in accordance with the company's business strategy and situation, such measures will only increase tasks, which might impact on day-to-day operation.

*Any outstanding risk not acceptable might give rise to unexpected loss.

Example of recommended actions

*Identify any risk involved in cyber-attacks (e.g. damage from leakage of important trade secret on strategical basis) that should be regarded as one of business risk in the course of business strategy exercise.

*Give direction to consider developing measures based on security level that should be attained against identified risk. At this point examine risk from the perspective of three factors (confidentiality, integrity and availability) of security while grasping dependency level on IT. As a result of this examination, execute risk management measures to the extent possible for the purpose of reducing averting and transferring risk (including use of cyber insurance or outsourcing asset protection to professional service providers). These types of measures include thorough update of software and reduction of malware infection risk such as implementation of software specialized in

malware prevention. Consider the introduction of multi-layer protective systems such as encryption of information and segregation of networks based on the differences of information assets with regards to terminals, networks and IT systems or IT services (including cloud service) with which important tasks are conducted.

(4) Publish cybersecurity measures framework (PDCA) and their actions.

Has a framework been built as PDCA for cybersecurity measures to execute and improve plans? And have directions been given to improve measures where necessary and to report the status of measures on a regular basis through execution of audit (or self-check)? Have directions been given to adequately reveal information on the status of measures to enhance trust of stakeholders?

Scenario in case of no action for security

*Without a framework that enables PDCA (Plan, Do, Check and Act), any plan might not be surely executed. It is also important to review security measures on a regular basis while understanding the status of cybersecurity measures in an organization with focus on addressing the latest threat. The failure in these efforts might lead to the inability to cope with changing cybersecurity, obsolescence of measures and difficulty to perform additional actions needed for new threat.

*Without proper disclosure of information on the status of measures, from the standpoint of social responsibility anxiety and distrust will arise from stakeholders in respect to business cybersecurity risk response, and it becomes impossible to deliver transparent explanation in case of risk occurrence. Degradation of trust of business partner and customer might cause compromise in the value of a company.

Example of recommended actions

*Develop a structure or process where one can constantly respond to a cybersecurity risk (assurance of implementation of PDCA). In the case where an organization has certain framework of PDCA on the internal governance, it can be combined with security measures for efficient execution.

*A committee on management risk (described in "Important Item 2") should provide opportunity to report to the management about the status of PDCA according to timeline and content set by a committee on management risk and also it should check if a new cybersecurity risk arises in a changing environment.

*Identify and resolve any issues regarding ongoing cybersecurity measures based on the result of audit where necessary.

*Give directions to promptly modify policy on risk as needed where a new cybersecurity risk is identified.

*Consider incorporating the report on the status of cybersecurity measures into other

reports such as information security report, CSR report, sustainability report and securities report in accordance with the nature or degree of risk set by cybersecurity measures.

(5) Make sure as to how group companies and business partners of the company's supply chain take security measures.

To secure a company's cybersecurity, it is vital that its group companies and business partners of the company's supply chain take proper security measures. Have directions been given to group companies and business partners of the company's supply chain to implement PDCA of cybersecurity measures including the execution of audit and the grasp of ongoing measures?

Scenario in case of no action for security

*Without any proper cybersecurity measures taken at group companies and business partners of the company's supply chain, the company might be targeted for attacks via these organizations vulnerable to attacks. As a result such company might be cause of collateral damage incurred by other companies or be responsible for damage incurred by other companies. Additionally, in an effort to identify cause of contingency, no cooperation from these companies means no smooth operation of business activities.

Example of recommended actions

*Conclude agreement or other documents on how group companies and business partners of the company's supply chain take security measures.

*Receive and grasp reports on how group companies and business partners of the company's supply chain take security measures.

3.3. Develop proactive measures to prevent cyber-attacks.

(6) Secure resource (budget, manpower etc.) to execute cybersecurity measures

Has a budget to implement cybersecurity measures been secured? And have directions been given to develop human resource and to provide proper treatment for them?

Scenario in case of no action for security

*Without any proper budget, it would be difficult to perform cybersecurity measures and obtain necessary manpower within an organization and also to entrust it with a reliable vendor.

*Without satisfactory treatment or improvement for personnel, it is impossible to retain talented human resource within an organization.

Example of recommended actions

*Give directions to specify cost needed to prepare identified proactive measures for cybersecurity.

*Provide continuous training on security by securing budget for trainings for not only personnel in charge of security but other employees.

*Obtain approval for budget after evaluating at a management meeting about whether or not expenditure is worth implementing measures.

*Consider using professional vendors in the event that it is hard to find human resource for cybersecurity within an organization.

*Give HR department directions to develop human resource for cybersecurity and to pave the way for career path in the course of human resource development efforts, and also to review what they work for these purposes.

(7) Identify the scope of outsourcing for system control and ensure cybersecurity in the applicable outsourcing companies.

To implement cybersecurity measures efficiently and steadily, have directions been given to appropriately divide task of IT system control based on the company's technical capabilities and degree of risk into that which the organization itself should take care of and that which outsourcing companies should handle? And assuming that outsourcing companies might be victimized by cyber-attacks when they are entrusted with work of IT system control, do you ensure that they have cybersecurity measures in place?

Scenario in case of no action for security

*No technical capability for IT system control within an organization might lead to insufficient system control, leaving vulnerability in the system, and eventually increasing possibility of cyber-attacks resulted from such vulnerability,

*In the case that outsourcing company's cybersecurity measures pose risk to the business, and ever if the outsourcing company implements security measures, the outsourcing company would be exposed by risk.

Example of recommended actions

*Review if the company can fulfill each security measure item on its own, taking note of its technical capability.

*Conclude agreements to confirm security levels of outsourcing companies to ensure they have adequate cybersecurity measures, and audit them based on the agreements.

*In case of entrusting outsourcing companies with important assets such as personal information or technical intelligence, conduct periodical verification of whether or not the entrusted assets are indeed secured, taking into account the business situation of outsourcing companies.

(8) Collect information on cyber-attacks through participation in information sharing activities, and develop environment to utilize such information.

Have directions been given to collect information on cyber-attacks through participation in information sharing activities and to develop environment to utilize such information so that one can deal with the latest cyber-attacks in the whole society?

Scenario in case of no action for security

*Information regarding the method of cyber-attacks found through participation in the information sharing activities can prevent damage from happening at other organizations. However without sharing information, one should respond to risk in the whole society every time new risk arises, which makes optimization on the whole impossible.

Example of recommended actions

*Guard against cyber-attacks in the whole society utilizing information shared by giving and taking of information. Provide actively information to help to guard against cyber-attacks through sharing information other than obtaining information.

*Make the best use of information from IPA and security alerts from JPCERT Coordination Center (general incorporated association) etc. for better cybersecurity measures.

*Make the best use of information sharing activities among CSIRT (Computer Security Incident Response Team) and collected information from participating in community activities hosted by Nippon CSIRT Association for better cybersecurity measures.

*Report information on malware and illegal access to the IPA in accordance with the public notification procedures (Standard of countermeasures for computer virus and Standard of countermeasures for illegal access to a computer).

*Provide information on incidents to JPCERT Coordination Center (general incorporated association), and request coordination where necessary.

*Utilize mechanism of information sharing of J-CSIP in the case of major infrastructure business.

3.4. Prepare in case of cyber-attacks occurrence

(9) Develop emergency response system (emergency contacts and initial action manual, CSIRT - Computer Security Incident Response Team), and execute regular and hands-on drill.

Have directions been given to develop an emergency response system including initial action manual, CSIRT, procedure enabling to normalize IT system and swift identification of influenced area and damage so that one can prevent further damage with a proper initial response? And have directions been given to carry out practical drill on a regular basis?

Scenario in case of no action for security

*Without development of system for emergency, there is no sharing information and no communication among relevant divisions and other external entities in conducting investigation of the cause of incident, and thus a swift work of identifying cause and emergency measures become impossible.

*At the time of emergency where things look different unlike ordinary times, it is in most cases difficult to follow the prescribed procedures smoothly. Emergency drills prepare personnel to act appropriately in unforeseen situations.

Example of recommended actions

*Build a structure or process for emergency in line with an organization.

*Give directions to promptly engage in cooperation with relevant organizations and to conduct a research on the log so that smooth actions or examination can be taken to identify a cause of damage after victimized by cyber-attacks. Moreover execute a drill in preparation of cyber-attacks for personnel in charge of response. It is recommended that such drill should include planning activities for the prevention of recurrence after incidents are under control.

*Prepare a list of emergency contacts. This list should include contacts such as system operation, Website maintenance/operation and contracted security vendors.

*Consider as to how an initial action should affect regular operation, and make arrangements in advance that enable prompt collaboration among relevant divisions (administration, planning, sales etc.) of an organization in times of emergency

*Execute a drill taking note of not only technical response but also preparation of press lease and submission of reports to the applicable government agencies.

(10) Collect information regarding contacts after damage is confirmed, and gather information to be disclosed, and prepare materials for the management's accountability.

Have directions been given to grasp contacts and information to be disclosed after incidents occur to swiftly deal with external entities? And have directions been given to develop a structure or process that enables the management's explanation to both internally and externally?

Scenario in case of no action for security

*Without a timely notification or security alerts, some damage might arise to customers and business partners, and also there might be responsibility of damage.

*Without a timely report to relevant government agencies that is mandatory under legal arrangements, it would cause penalty or punishment.

*Without an announcement about computer virus infection from the management who spearhead information management function, responsibility as an organization would not be discharged to stakeholders.

Example of recommended actions

*Prepare a format used for a list of contacts and notification and share them with personnel in charge of response so that it will become possible to send promptly notifications or security alerts after detecting damage due to cyber-attacks. And make sure of how related information is disclosed.

*Verify a procedure by which one can comply with the relevant laws and discharge legal obligations.

*Let the management know about the status of damage and impact to other companies due to incidents so as to publish incidents internally and externally upon the request made to the management.

*Publish promptly incidents taking an account of their impact on stakeholders.

*Publish incidents in a timely manner depending on the status of the damage from incidents at such times as the early stage of incidents, the grasp of damage and the incidents under control.

Appendix A Check sheet of cybersecurity management

∗ This check sheet requires additional items according to the situation of each company as it lists only basic items for cybersecurity management.

(1) Recognize a cybersecurity risk and develop company-wide measures.

□ The management regard a cybersecurity risk as one of management risks.

□ Develop and publish policy on company-wide measures (security policy) taking cybersecurity risk into consideration.

(2) Build a structure or process for a cybersecurity risk management.

□ A structure or process for cybersecurity risk management such as CISO is built according to the policy on company-wide measures.

□ Responsibility of each personnel in a structure of cybersecurity risk management is defined.

□ The relationship between a structure of risk management and a structure of cybersecurity risk management is defined.

(3) Determine goals and develop plans based on perception of a cybersecurity risk and security level that should be attained.

□ Assets to be protected are specified.

□ Threat of cyber-attacks against the specified assets is identified and recognized as cybersecurity risk specified in the business strategy.

□ How cybersecurity risk affects the business is foreseen.

□ Goals or plans are developed to mitigate or avert risk in accordance with the degree of impact of individual cybersecurity intrusions.

□ Company has transferred cybersecurity risks it decided not to take measures for reducing and averting. (e.g. by using cyber insurance or outsourcing asset protection to professional service providers)

□ Determine what level of cybersecurity risk can be left as an outstanding risk due to its impact without implementing risk aversion.

(4) Publish cybersecurity measures framework (PDCA) and their actions.

□ Reports on how group companies and business partners of the company's supply chain take security measures are provided to the management and grasped by

them on a regular basis.

□ An external audit is conducted for a cybersecurity risk.

□ Review is conducted for risk or threat of a cybersecurity where necessary, and a response system in line with the changing environment (PDCA) is developed and maintained.

□ The status of response efforts and a cybersecurity risk is published externally.

(5) Make sure as to how group companies and business partners of the company's supply chain take security measures.

□ Reports (including audit) on how group companies and business partners of the company's supply chain take cybersecurity measures are provided and grasped.

(6) Secure resource (budget, manpower etc.) to execute cybersecurity measures.

□ Required cybersecurity measures are defined, and a budget after evaluating at a management meeting about whether or not expenditure is worth implementing measures is secured.

□ Human resource is secured for cybersecurity measures (both internally and externally).

□ Human resource is developed and trained in an organization.

□ Career path is internally built for personnel in charge of cybersecurity, and they are properly treated.

□ Training on security by securing budget for trainings for not only personnel in charge of security but other employees is provided on a regular basis.

(7) Identify the scope of outsourcing with IT system control and ensure cybersecurity in the applicable outsourcing companies.

□ Appropriately divide task of IT system operation into that which the organization itself should take care of and that which outsourcing organizations should handle.

□ Cyber-attacks against outsourcing companies is foreseen and cybersecurity at outsourcing companies is secured.

(8) Collect information on cyber-attacks through participation in information sharing activities, and develop environment to utilize such information.

□ Information sharing is conducted based on security alerts on cybersecurity given by various organizations or through the participation in relevant communities, and such sharing contributes to the company's measures.

□ Upon receiving information on malware and illegal access, and in the case of incident occurrence, submitting a report to IPA and providing information to JPCERT Coordination Center (general incorporated association) is properly conducted, and providing information to a mechanism of information sharing promoted by other independent organizations is also conducted.

(9) Develop emergency response system (emergency contacts and initial action manual, CSIRT - Computer Security Incident Response Team), and execute regular and hands-on drill.

□ A list of emergency contacts and a communication chart are completely prepared (emergency contacts include contacts such as system operation, Website maintenance/operation and contracted security vendors).

□ An initial action manual for cyber-attacks is developed as with disasters.

□ A dedicated incident response team (CSIRT etc.) is established.

□ A post-incident plan is properly made, and a regular response drill is conducted on a regular basis.

(10) Collect information regarding contacts after damage is confirmed, and gather information to be disclosed, and prepare materials for the management's accountability.

□ A list of contacts for communication to external entities (including stakeholders and the relevant government agencies) is completely prepared.

□ Information to be disclosed and reported is properly grasped and organized.

□ A contact chart for report to the management and the content / time schedule of what should be published are considered in advance so that the management can give a necessary account of the situation both internally and externally.

Appendix B Recommended technical measures and reference documents (Note: These are examples as of now and subject to change in accordance with the change of environment or the status of each company.)

The management and personnel with information system division in charge of technical measures should have common recognition about the following items, risk of no action for security, and the management are recommended to consider making arrangements for resource needed to execute measures at the discussion / request of the relevant divisions.

Examples of technical measures are otherwise listed in "Appendix B-2." Personnel with information system division are asked to refer to it for detailed information.

Individual management guidelines	Technical measures for realization of each item	Risk of no action, Result from implementation	Reference documents, Information, Tool
(3) Determine goals and develop plans based on perception of a cybersecurity risk and security level that should be attained.	**Identify assets to be protected, Grasp risk** Identify assets to be protected as an organization which should comply with the industry's safety standard as well as the applicable laws in the course of the business, and grasp an internal network system and risk due to its use.	・ Without identifying assets to be protected (important information or personal information), it is impossible to swiftly respond to emergency with focus on the priority of the assets. ・ No grasp of an internal network system might mean inability to adequately protect important information, leading to a waste of time as well as more damage, and also mean inability to identify the scope of damage and to look for the cause of an incident, leading to prolonged situation.	
	Perform multi-layer protective system Perform "a multi-layer protective system" which enables multiple measures to prevent malware infection as well as to avert or minimize damage caused by infection.	・ The only infection preventing measures (anti-malware software etc.) might not work well in the case of unknown malware, resulting in the inability to prevent damage from spreading further. ・ It is necessary to take security measures for the whole network system rather than depending on an individual security by implementing an anti-malware software or firewall on network exit, and also is important to have flexible measures to enable	<Information> "System design guide for responding to 'advanced targeted attack' " by IPA "Security alerts - Recommendation on security measures and operation management in preparation of virus infection - June 2, 2015" by IPA "10 Major Security Threats 2014 (Chapter 1 Basics of measures)" " Guidelines for the Prevention of Internal

		prevention or mitigation of damage in such way as to deal with attack phases of invasion, infection and spread. ・ If a regular check by internal or external monitoring provider is not conducted to the device (which records and saves various logs) installed at the network exit, it is impossible to detect illegal communication.	Improprieties in Organizations" <Information> "Use and method of analysis of log in relation to response against advanced cyber attack" by JPCERT/CC "iLogScanner" by IPA
(4) Publish cybersecurity measures framework (PDCA) and their actions.	**Perform and improve PDCA cycle** Review improvements of current security measures, and design / execute future improved plans based on PDCA cycle performed by ISMS or security audit.	・ Without any review of measures or constant improvement in line with changing environment or business, it might be impossible to respond to new threats.	<Scheme/System> "Information Security Management System (ISMS) Conformity Assessment Scheme" by JIPDEC "Cybersecurity Management System (CSMS) Conformity Assessment Scheme" by JIPDEC "Audit system on information security" by Ministry of Economy, Trade and Industry <Tool> "Benchmark on information security measures" by IPA

	<u>Perform security diagnosis</u> Perform and review measures for existing vulnerability by utilizing vulnerability diagnosis services of Web applications and platforms provided by professional service providers or tools as well as executing review security measures internally.	・ As much vulnerability is detected and many security patches become available on a daily basis, a larger IT system might cause failure in measures. ・ Without any regular check to find defect in security, the grasp and the response of such defect would be late, and it might create a chance for third parties to abuse IT system, causing damage by malware infection etc.	<Reference documents> "How To Secure Your Web Site" (and supplement "Web site check") by IPA "Introduction of inspection method of vulnerability in web site (web application inspection)" <Tool> IPA MyJVN Version checker <Reference> "JNSA Solution Guide" by JNSA
(5) Make sure as to how group companies and business partners of the company's supply chain take security measures.			<Information> "Guidelines on the promotion of the improvement of subcontracting transactions in information service/software industry" by Ministry of Economy, Trade and Industry "Guide for information security management with supply chain" by JASA
(6) Secure resource (budget, manpower etc.) to execute cybersecurity measures.			<Information> "Skill index for strengthening information security" by IPA "Guide for developing human resource in charge of information security with the use of IT skill index" by IPA

			"Study on development of information security managers at workplaces" Benchmark on information security measures" by IPA
(7) Identify the scope of outsourcing with IT system control and ensure cybersecurity in the applicable outsourcing companies.	**Appropriately divide task which the organization itself should take care of and task which outsourcing organizations should handle.** Assuming that what is technically hard for the organization itself to conduct an inspection on devices such as infected terminals should be handled with the support of external professional entities or security vendors, divide tasks in advance into (i) what the organization itself can do and (ii) what should be entrusted with to external entities. And secure budget for that purpose in advance.	・ The difficult situation in executing measures by the organization itself and no advanced analysis for incidents would mean no ability to investigate the cause as well as no ability to decide the scope of damage, eventually allowing incidents to further continue, otherwise secondary or tertiary attack to be delivered.	
(8) Collect information on cyber-attacks through participation in	**Utilize information collected through participation in information sharing activities and information provided by public sector.**	・ The domain of cybersecurity is making rapid progress for cyber-attackers or defenders. Without a regular collection of information on the latest attack technique, the organization itself will be unable to decide what level of measures should be taken.	<System etc.> "Notification of compute virus, illegal access and vulnerability related information" by IPA "Special help desk for targeted cyber-attacks" by IPA

information sharing activities, and develop environment to utilize such information.	Participate in information sharing activities with cyber-attacks and utilize information provided by public sector or professional service providers to find out if measures against cyber-attacks are properly developed (where or not measures are at the ordinary level). Provide actively information to others as well as receiving it.	・ Insufficient efforts in information sharing activities or participation in information sharing communities might result in degradation of response ability of the industry on the whole.	"Cyber information sharing initiative (J-CSIP)" by IPA "Report on incidents," "Provision of early warning information," Nippon CSIRT Association" by JPCERT/CC "@police" by National Police Agency https://www.npa.go.jp/cyberpolice/
(9) Develop emergency response system (emergency contacts and initial action manual, CSIRT - Computer Security Incident Response Team), and execute regular and hands-on drill.	**Develop a structure or process in times of emergency and prepare for identification of damage.** ・ Build mechanism to make it possible to detect and record cyber-attacks on a daily basis and prepare response procedure at the time of detecting attacks. ・ Identify completely the scope of impact and damage, and establish procedures for the normalization of network, escalation to the management and contact routes.	・ Without any structures or process for incident response and procedures for contacts or report, personnel cannot recognize cyber-attacks or personnel can be only slow to decide the degree of damage, or decide when to disengage PC or terminal, when to disconnect internet, and as a result one would fail to complete an initial action, which causes a delay in the return to normal state in regular work or services, eventually would be exposed to social responsibility, law suit, and would lead to degradation of trust. ・ The remaining infected terminal or malware would be the cause of the recurrence of information leakage, making the incident continue further.	<Development of structure or system> JPCERT/CC "Material for building CSIRT" Nippon CSIRT Association "CSIRT Starter Kit" <Detection of cyber-attack / Identification of damage> "Conduct inspection on the potential malware infection" by IPA "Security alert on illegal use of domain administrator account with Active Directory" by JPCERT/CC "Use and method of analysis of log in relation to

	・ Determine impacted area with not only function of device or software but also security experts. ・ Establish a help desk or procedure to respond to inquiries regarding attacks or damage from external organizations or to provision of information from them...	・ Unless an appropriate log is saved for a reasonable period at an appropriate device even if communication with external device is confirmed, it is impossible to ascertain the scope of damage as to how further and when devices are infected.	response against advanced cyber-attack" by JPCERT/CC
	Perform regular drill for personnel Perform drill for incident response and targeted attack. Ensure that discovery of spam mail should be reported to the applicable desk rather than accusation of opening it.	・ Without any drill in preparation for incident, attackers can easily invade a system. ・ It should be recognized that a targeted mail can be inevitably opened. Accusation of opening a spam mail at the training session might lead to more damage due to unwillingness to report spam mail upon the actual receipt.	

Appendix C In relation to International Standard ISO/IEC 27001 and 27002

	ISO/IEC27001(x), ISO/IEC27002(-)
(1) Recognize a cybersecurity risk and develop company-wide measures.	x 5.1 Leadership and commitment x 5.2 Policy
(2) Build a structure or process for a cybersecurity risk management.	x 5.3 Organizational roles, responsibilities and authorities - 6.1.1 Information security roles and responsibilities
(3) Determine goals and develop plans based on perception of a cybersecurity risk and security level that should be attained.	x 6.1 Actions to address risks and Opportunities x 6.2 Information security objectives and planning to achieve them - 5.1.1 Policies for Information security - 5.1.2 Review of the policies for information security
(4) Publish cybersecurity measures framework (PDCA) and their actions.	x 7.4 Communication x 8.1 Operational Planning and control x 8.2 Information security risk assessment x 8.3 Information security risk treatment x 9.1 Monitoring, measurement, analysis and evaluation x 9.2 Internal audit x 9.3 Management review x 10.1 Nonconformity and corrective action x 10.2 Continual improvement - 17.1.1 Planning information security continuity - 17.1.2 Implementing information security continuity - 17.1.3 Verify, review and evaluate information security continuity - 18.1.1 Identification of applicable legislation and contractual requirements - 18.2.1 Independent review of information security - 18.2.2 Compliance with security policies and standards - 18.2.3 Technical compliance review
(5) Make sure as to how group companies and business partners of the company's supply chain take security measures.	x 8.1 Operational Planning and control
(6) Secure resource (budget, manpower etc.) to execute cybersecurity measures.	x 7.1 Resources x 7.2 Competence
(7) Identify the scope of outsourcing with IT system control and ensure cybersecurity in the applicable outsourcing companies.	- 6.1.3 Contact with authorities - 6.1.4 Contact with special interest groups
(8) Collect and utilize information on cyber-attacks through participation in information sharing activities, and develop environment to utilize such information	- 6.1.3 Contact with authorities - 6.1.4 Contact with special interest groups
(9) Develop emergency response system (emergency contacts and initial action manual, CSIRT - Computer Security Incident Response Team), Execute regular and hands-on drill.	- 16.1.1 Responsibilities and procedures - 16.1.2 Reporting information security events - 16.1.3 Reporting information security weaknesses - 16.1.4 Assessment of and decision on information security events - 16.1.5 Response to information security incidents
(10) Collect information regarding contacts, and gather information to be disclosed, and prepare materials for the management's accountability.	- 6.1.3 Contact with authorities - 6.1.4 Contact with special interest groups

Appendix D Definition of terms

(1) Incident

A state of affairs in which a cybersecurity risk is realized or materialized.

(2) Audit

A systematic, independent and documented process for collecting evidence and objectively determining whether or not cybersecurity measures are appropriately implemented in an organization. An audit can be executed either internally (primary) or externally (secondary or tertiary) or through a combination of internal and external audits.

(3) Cyber-attack

Any attack with malicious intent which invades illegally into computer system or network to steal or destroy or execute unauthorized program.

(4) Cybersecurity and Cybersecurity risk

Cybersecurity is an effort to prevent information leaks or IT system malfunctions which occur due to cyber-attacks. Cybersecurity risk is corporate management's measurement of the possibility of such problems occurring.

(5) Outstanding risk

Any risk which stays after response (aversion, reduction, transfer of risk) for risk is finished. It may be referred to as risk acceptance.

(6) Information security

Information security is intended to maintain confidentiality, integrity and availability.

(7) Information security report

A report which discloses the security situation of a company, which is meant to allow companies to be properly evaluated by such stakeholders as customers and investors. This report tends to attract public attention.

(Reference: "Model for information security report" by Ministry of Economy, Trade and Industry:
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf)

(8) Stakeholder

Persons or organizations that can affect, can be affected by, or are aware of being affected by company's decision making or actions. In other words they are shareholders, creditors, customers and business partners.

(9) Security policy (Basic policy of information security)

Security policy is developed by the management to officially express their objectives and views on information security in organizations. Security policy contains the provisions of security measures in organizations.

(10) Multi-layer protective system

It is expected that the introduction of a multi-layer protective system including physical layer, network layer and data layer will help to reduce risk of breach by unknown malware or new type of attack more smoothly than depending on a single point defense such as single device or software or depending on a single perimeter protective system (mainly network perimeter).
IPA recommends the following four points as examples of multi-layer protective measures. (i) Reduction of software infection risk (ii) Segregation of terminals and networks (iii) Restricted access on server with important information (iv) Preparation for post-incident

(11) Business partner

Companies with which any company has business relationships such as outsourcing or procurement of goods or services.

(12) Malware

It is collectively referred to any malicious programs that cause damage to information security including computer virus, spyware and bot. These programs perform malicious actions by invading a computer against the will of users or administrators (or before they become aware of it).

(13) Risk

International Standard (ISO/IEC 27000 defines "risk" as "impact of uncertainty against various objectives."

(14) Risk response (aversion, reduction, transfer and acceptance)

Ways to respond to risk largely include four responses of "risk aversion," "risk reduction," "risk transfer" and "risk acceptance." According to JISQ0073 Risk Management - Vocabulary, these risk responses are categorized into seven elements such as risk aversion, risk taking or

increasing to gain opportunity, elimination of risk reduction, alternation of risk likelihood, change of result, risk transfer, risk acceptance.

(i) Risk aversion

"Risk aversion" means that possibility of risk occurrence should be eliminated by removing factor of risk occurrence or taking other method. This can be illustrated by the case in which publication of web sites is suspended to disconnect with external communication "against threat of illegal invasion on the internet."

(ii)Risk reduction

"Risk reduction" means that possibility of threat should be reduced by taking measures of information security against vulnerability. It includes such methods as encrypting information to be saved against loss, theft and leakage, and ensuring control of access to server rooms using biometric identification technique against illegal invasion, and providing training on information security to personnel.

(iii)Risk transfer

"Risk transfer" means that risk should be transferred to other companies or organizations. It includes such methods as claiming damages with insurance policy when risk becomes apparent, and outsourcing the operation of internal information system through contracts with other companies to claim damages due to illegal invasion or malware infection based on these contracts.

(iv)Risk acceptance

"Risk acceptance" means that potential loss should be accepted depending on the nature of certain risk.

(15) Risk assessment

Process in which result of risk analysis is compared with risk criteria (which acts as reference to evaluate risk based on objectives and internal/external environment of organizations) to determine where or not the size of risk is acceptable.

(16) Risk analysis

Process through which one can apprehend the nature of risk and determine level of risk (size of risk based on combination of result and likelihood of an incident).

(17) Log

It is a record to contain use of computers or communication history of data. Log contains ID of users, date operated and operation itself etc. Log is used to identify cause of incident as regards to information security.

(18) CISO (Chief Information Security Officer)

The responsible person designated from among the management or appointed by a top executive to perform information security measures.

(19) CSIRT (Computer Security Incident Response Team)

This is the name of the team which is responsible for tackling incidents described in these guidelines.

Reference:

CSIRT Building materials for response team JPCERT Coordination Center (general incorporated association) https://www.jpcert.or.jp/csirt_material/

Nippon CSIRT Association http://www.nca.gr.jp/

CSIRT Starter kit (Nippon CSIRT Association)

http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

CSIRT Reference material useful for building response team (Nippon CSIRT Association)

http://www.nca.gr.jp/activity/build-wg-document.html

(20) PDCA

This is the acronym for Plan - Do - Check - Act. This is a well-known methodology to maintain improvement reiterating the following steps.

1. Plan: Make plans to accomplish a target determined after sorting out issues.
2. Do: Perform actual work based on a target and its plans.
3. Check: Verify and evaluate whether or not the initial target was accomplished in accordance with plans.
4. Act: Improve the work based on the result of evaluation.