Cybersecurity Management Guidelines

Ver. 2.0

Ministry of Economy, Trade and Industry (METI)

Information-technology Promotion Agency, Japan (IPA)

Contents

Outline of the Cybersecurity Management Guidelines

I. Cybersecurity is a business management issue.

- The use of IT in companies does not only simply improve companies' profitability by streamlining operations but also it has become an essential requirement for companies to be able to compete in the global market. Furthermore, with technologies such as IoT that create new value becoming increasingly common, companies are required to create new products and services utilizing AI and big data, and establish corporate value and business with global competitiveness.

- Cyber-attacks are becoming increasingly advanced and sophisticated every year and incidents have been occurring that cause serious impact, such as companies losing over half of their net profits due to cyber-attacks.

  Not only have such attacks been affecting each company's business, there have also been attacks with the potential to cause significant impact on the social lives of the people, such as the leakage of sensitive technical information for the security of the country or the suspension of important infrastructure services. The threat of such attacks are increasing.

- If corporate management does not conduct appropriate security investment and causes damage to society, there is a possibility of society questioning their response to risk, or even their management responsibility or legal liability. Additionally, the necessity of security measures in the supply chain has increased both in Japan and abroad, and the possibility for outsourcing companies to have impact on international business is emerging.

- Moreover, security investment has become something that is not limited to securing business continuity or improving defense against cyber-attacks, but an essential element in generating companies' revenue utilizing IT. It is important to consider the implementation of security measures not as costs, but to position them as investments that are necessary for future business activities and growth.

- In the current situation in which cyber-attacks have become a risk that cannot be avoided, investment in security as a management strategy has become a necessary and indispensable responsibility of business managers.

- These guidelines are aimed at the corporate management of major companies as well as small and medium-sized companies (excluding small-scale enterprises) and include, from the viewpoint of protecting companies from cyber-attacks, the three principles which management needs to recognize and ten important items which management should direct their executive in charge (CISO) to observe in implementing cybersecurity measures.

II. Three principles which management needs to recognize

It is essential that management recognizes the following three principles and drives measures.

1. Corporate executives need to recognize cybersecurity risks and take leadership in driving cybersecurity measures.

   (Management should take leadership to drive cybersecurity measures taking into account the risks of cyber-attacks and their impact on the company while also conducting security investment for the growth of their company.)

2. Security measures need to be taken not only for the company itself but also for the supply chain including business partners and outsourcing companies.

   (Cybersecurity measures should be applied not only to the company itself but also to its business partners and outsourcing companies in the supply chain.)

3. Companies need to communicate appropriately with relevant stakeholders by, for example, disclosing information on cybersecurity risks and measures in normal time as well as in time of emergency.

   (Management should foster relationships of trust with relevant people including stakeholders (clients, shareholders, etc.) in normal time by conducting information disclosure related to cybersecurity measures to prepare for smooth communication even when incidents occur.)

(For details, refer to 2. Three principles which management needs to recognize below.)

III. Ten important items of cybersecurity management

Management should instruct the executive in charge of implementing cybersecurity measures (CISO etc.) on the following ten important directions.

Direction 1 : Recognize cybersecurity risk and develop a company-wide policy

Direction 2 : Build a management system for cybersecurity risk

Direction 3 : Secure resources (budget, workforce etc.) for cybersecurity measures

Direction 4 : Identify cybersecurity risks and develop plans to address them

Direction 5 : Establish systems to effectively address cybersecurity risks

Direction 6 : Implement a PDCA cycle for cybersecurity measures

Direction 7 : Develop a cybersecurity incident response team and relevant procedures

Direction 8 : Develop a recovery team and relevant procedures in preparation for damage due to cyber incidents

Direction 9 : Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies

Direction 10 : Gather, utilize, and provide cyber-threat information through information sharing activities

(For details, refer to 3. Ten important items of cybersecurity management below.)

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 technical information owned by companies, or to shut down their systems, and about 40 percent of companies have experienced cyber-attacks (see Fig. 1). However, it is likely that many victim companies are not aware of being damaged by cyber-attacks, which is indicated by the fact that about half of reported incidents on cyber-attacks are reported by external entities. While there have been many attacks in which the damage is immediately noticed such as ransomware attacks, targeted attacks aimed at stealing information are difficult to detect unless appropriate security measures are in place. Therefore, it is unthinkable for a company not to conduct security investment until it finds itself the victim of a cyber-attack.

Furthermore, in addition to office computers, as more and more computers in social infrastructure and factory control systems etc. get connected to external networks, the impact of cyber-attacks are reaching physical environments.

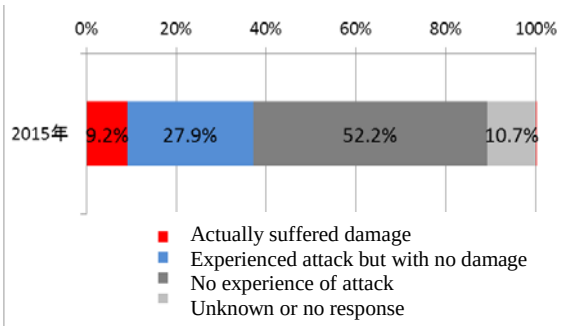

Fig. 1 **Ratio of companies that suffered damage by cyber-attacks (excluding computer virus)** [1]

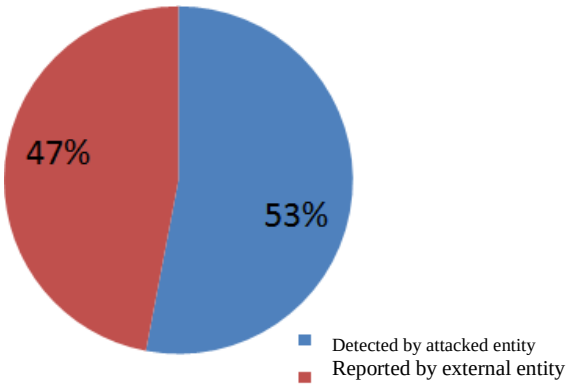

Fig. 2 **How a security breach was detected**[2]

In this way, while we have witnessed the increasing threat of cyber-attacks directed at companies, we cannot be assured that many companies are committed to measures to addressing them. One of the reasons might be that management has insufficient capabilities as leaders to deal with cybersecurity measures. Less than 20 percent of companies consider security investment as investment for future growth in their distribution of management resources and an overwhelming majority of companies consider security investment to be unavoidable expenses. Additionally, of the companies that consider security investment to be investment for future growth, over 70 percent have

secured the necessary security budget, but among the companies that consider it unavoidable expenses, the ratio is around 40 percent.

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 the Ministry of Economy, Trade and Industry based on "M-Trends 2017: Perspective of security measures forefront" by FireEye Inc.

This indicates that when management takes leadership to conduct security investment for the growth of their company, it leads to improving the company's resistance to cyber-attacks.

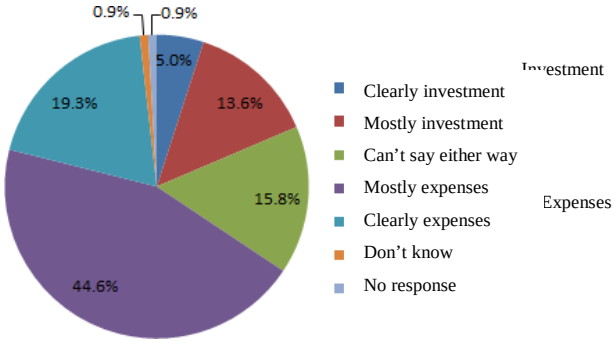

Fig. 3 **Positioning of security measures expenditure (expenses or investment)[3]**

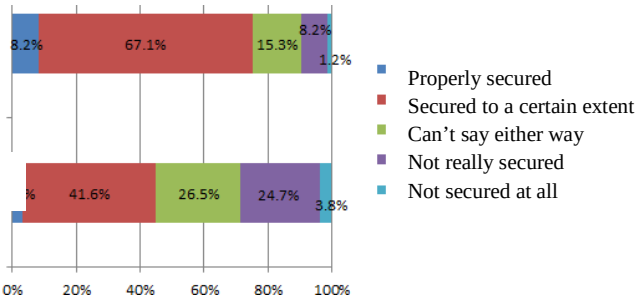

Fig. 4 **Securement of the necessary security budget[3]**

One of the most essential roles that management should fulfill is, for proactive investment to improve corporate value and competitiveness, firstly to recognize the value and role of systems essential for their business operation and important information such as trade secrets in the context of corporate strategy, and secondly to make a clear policy for cyber risks. When conducting IT investment, it is necessary to simultaneously consider security investment in preparation for such cybersecurity risks; in order to improve corporate value, management must take leadership and consider cybersecurity within the overall corporate strategy. If the development of such corporate strategy is neglected, the use of IT aimed at improving corporate value could, as a result, cause serious damage and develop into a situation that could affect the management of the company.

Against this backdrop, the Cybersecurity Management Guidelines were developed to collectively publish principles of cybersecurity that management should follow and items that should be undertaken under their leadership as companies drive the use of IT. Specifically, these guidelines include contents on how to drive organization and measures relating to security risks under the leadership of 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 conduct appropriate investment for cybersecurity and enhance their company's cybersecurity measures under their leadership.

These guidelines are also targeted at major/medium/small businesses (excluding tiny businesses). 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 and should be applied in accordance with the situation of each company.

3. Prepared by the Ministry of Economy, Trade and Industry based on "Security Survey 2017" by KMPG Japan

Additionally, small / medium businesses that are considering efforts for cybersecurity measures going forward should also refer to the Guidelines for IT Security Measures for Small and Medium Sized Businesses.[4]

Ver. 1.0 and Ver. 1.1 of these guidelines have been put together based on the results of an exploratory session titled "Study on cybersecurity risk and corporate management" and Ver. 2.0 based on the "Study on the revision of the cybersecurity management guidelines," jointly sponsored by the Ministry of Economy, Trade and Industry and the Information Technology Promotion Agency (independent administrative institution) (hereafter "IPA") respectively. 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 recommended to utilize this document together with the Cybersecurity Management Guidelines as it is the document from which the basic idea of these Guidelines is derived.

---

4 Guidelines for IT Security Measures for Small and Medium Sized Businesses (IPA) https://www.ipa.go.jp/security/keihatsu/sme/guideline/

5 Approaches to cybersecurity for corporate management (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. The top summary is intended for management. Chapters 2 and 3 are intended for executives responsible for cybersecurity measures (CISO) or personnel responsible for security.

Outline of the Cybersecurity Management Guidelines

1. Introduction
2. Three principles which management needs to recognize
3. Ten important items of cybersecurity management

(Appendix)

A) Check sheet of cybersecurity management
B) Reference material on cybersecurity measures
C) Items to organize within an organization when an incident occurs (Separate sheet)
D) In relation to International Standard ISO/IEC 27001 and 27002
E) Definition of terms

Management should review at least the overview, recognize the three principles and subsequently give instructions on the ten important items to the CISO.

The CISO should drive security tasks based on instructions from management by giving more detailed instructions to personnel in charge of security while referring to the examples of measures described in explanatory pages regarding the ten important items.

Additionally, appendices are included in these Guidelines as reference for the implementation of the ten important items. The contents of each appendix are as follows.

Appendix A	Check sheet to confirm whether the ten important items are being implemented appropriately
Appendix B	Reference material for implementing cybersecurity measures
Appendix C	Items to organize within an organization in investigating the cause when an incident occurs
Appendix D	Relationship between the ten important items and ISO/IEC27001 and 27002
Appendix E	Definitions of the terms used in these Guidelines

For risks of internal threats such as leakage of information committed by employees, “Guidelines for the Prevention of Incidents by Internal Threats”[6] written by the IPA will be helpful for effective actions.

“Guidelines for IT Security Measures for Small and Medium Sized Businesses” by

the IPA will also serve as reference for companies that are planning to start making efforts for cybersecurity measures.

6. Guidelines for the Prevention of Internal Improprieties in Organizations (IPA) https://www.ipa.go.jp/files/000044615.pdf

2. Three principles which management needs to recognize

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

(1) Corporate executives need to recognize cybersecurity risks and take leadership in driving cybersecurity measures.

(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 their fate.
- For this reason it is vital that management should position cybersecurity risks as an important factor in risk management and appoint an executive in charge (CISO, etc.) of implementing cybersecurity measures, while at the same time utilize their leadership and distribute appropriate resources to take the necessary countermeasures against cybersecurity risks.

(2) Security measures need to be taken not only for the company itself but also for the supply chain including business partners and outsourcing companies.

(Explanation)

- In the case that there are cyber-attacks on business partners or outsourcing companies (for example, system management service providers), the concern arises that information provided by the company might be compromised.
- Therefore, comprehensive security measures are necessary to cover the company itself, business partners and outsourcing companies in the company's supply chain.

(3) Companies need to communicate appropriately with relevant stakeholders by, for example, disclosing information on cybersecurity risks and measures in normal time as well as in time of emergency.

(Explanation)

- By constantly communicating with relevant parties in normal time, distrust or anxiety among parties can be subdued even in case of emergency.
- Thus companies need to continue communication with relevant parties or partners in normal time to let them know that the necessary cybersecurity measures are in place.

3. Ten important items of cybersecurity management

Management is required to steadily drive cybersecurity measures by giving the CISO instructions on the following ten important items as well as receive regular reports from the CISO on the implemented measures. For items that are difficult to handle within the organization itself, implementation through outsourcing should be considered.

<Drive security measures under the leadership of management>

(Build a structure or process for cybersecurity risk management)

Direction 1: Recognize cybersecurity risk and develop a company-wide policy

Direction 2: Build a management system for cybersecurity risk

Direction 3: Secure resources (budget, workforce etc.) for cybersecurity measures

(Identify cybersecurity risks and implement measures)

Direction 4: Identify cybersecurity risks and develop plans to address them

Direction 5: Establish systems to effectively address cybersecurity risks

Direction 6: Implement a PDCA cycle for cybersecurity measures

(Establish a system to prepare for the occurrence of incidents)

Direction 7: Develop a cybersecurity incident response team and relevant procedures

Direction 8: Develop a recovery team and relevant procedures in preparation for damage due to cyber incidents

<Drive security measures in the supply chain>

Direction 9: Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies

<Drive communication with stakeholders and other relevant parties>

Direction 10: Gather, utilize and provide cyber-threat information through information sharing activities

3. 1. Build a cybersecurity risk management system

Direction 1　Recognize cybersecurity risk and develop a company-wide policy

Recognize cybersecurity risk as one important element among a variety of management risks and develop a company-wide policy (security policy).

Scenario in case of no action

- Without cybersecurity policy developed and announced by management, each security measures implemented will be inconsistent with the corporate strategy.
- This act of announcing them will heighten the trust of stakeholders such as shareholders, customers, and business partners, leading to the increase in value of the brand. However, without such an act, there is no enhancing trust as the degree of importance of cybersecurity in the company is not conveyed to the stakeholders.

Examples of recommended actions

- Develop a security policy taking cybersecurity risks into consideration while aligning it with the management policy of the company so that management can announce the organization-wide policy to inside and outside the organization. When doing so, consider a response policy that takes into consideration not only information systems but also business such as manufacturing, sales, services etc..
- The security policy should be posted somewhere that is easily accessible to employees (such as an internal portal site) and management should ensure that employees are thoroughly familiar with the policy by conducting employee education and other methods.
- By publicly announcing the security policy, the company will be able to show its security posture to stakeholders and society and increase trust from them.

Direction 2 Build a management system for cybersecurity risk

Establish a structure for cybersecurity risk management (including defining the responsibility of each relevant person) in order to implement cybersecurity measures. In doing so, make sure that such structure is consistent with other risk management structures within the organization.

Scenario in case of no action for security

- Without a structure for cybersecurity risk management, it is impossible to identify cybersecurity risks as a whole company.
- Unless the cybersecurity risk management structure is aligned with other risk management structures within the organization, there is a risk of inconsistency between the cybersecurity risk management policy and the overall risk management policy.

Examples of recommended actions

- The CISO should establish a cybersecurity management structure and define its scope of responsibility.
- The CISO should participate in a corporate risk management committee in the organization.
- The directors and auditors should audit such cybersecurity risk management structure to check if it is properly established and works accordingly.
- Based on the concept of “Security by Design”, the cybersecurity risk management structure should cover plan / design phase as well as later phases (operation etc.).

Direction 3 Secure resources (budget, workforce etc.) for cybersecurity measures

Secure the budget to implement measures for cybersecurity risks and provide training for cybersecurity personnel.

Scenario in case of no action for security

- Without a proper budget, it would be difficult to implement cybersecurity measures and obtain the necessary workforce within an organization or to outsource it to a reliable vendor.
- Without providing satisfactory treatment for security personnel, it is impossible to retain talented human resources within an organization.

Examples of recommended actions

- Identify the necessary cybersecurity measures and secure the budget necessary for them.
- Secure a budget for training of employees and personnel in charge of security and provide constant training in accordance with their roles.
- Consider using professional vendors if it is hard to find human resources for cybersecurity within the organization.
- Consider developing internal human resources for cybersecurity[7] including hiring external resource, and designing a career path for them, as part of the organization's IT human resources development strategy.
- Consider using security training provided by external organizations[8] if it is hard to train human resources for cybersecurity within the organization.

7. (Reference) Using systems such as specialist certifications offered by private companies or the Registered Information Security Specialist Examination administered by the IPA is effective as an indicator to measure the skills of security personnel.

8. (Reference) The IPA also offers programs to train security personnel engaged in work related to information and control systems for social infrastructure and the industrial base (Industrial Cyber Security Center of Excellence)

3. 2. Identify cybersecurity risks and implement measures

Direction 4　　Identify cybersecurity risks and develop plans to address them

Identify information that should be protected from the perspective of corporate strategy, identify cybersecurity risks from the threat of cyber-attacks and level of its impact, and develop a plan for such risks.
In that process, consider measures of risk transfer (cyber insurance, outsourcing etc.) and finally identify residual risks

Scenario in case of no action for security

- Without proper risk management measures in accordance with each company's business strategy and situation, such measures will only increase tasks, which might impact day-to-day operations.
- Any unacceptable risk remaining might cause unexpected loss.

Examples of recommended actions

- Of all the information in the organization, identify and locate information that should be protected from the perspective of corporate strategy.
- Identify cybersecurity risks related to the information that should be protected (for example, damage due to leakage of trade secrets essential to corporate strategy).
- Consider cybersecurity measures for the identified risks from the following perspectives.

  -- Implementation of risk reduction measures (measures to lower the probability of the risk occurring)

  Example: thorough access control to important information and software updates

  -- Implementation of risk avoidance measures (measures to eliminate the possibility of the risk occurring) Example: prohibit taking a laptop to outside the company (avoid the risk of theft outside the company)

  -- Implementation of risk transfer measures (measures to transfer risks to other entities, etc. Example: using cloud services, purchasing cyber insurance)
- Identify residual risks for which measures are thought to be unnecessary based on their probability of occurrence and level of potential damage.
- Consider legal requirements about protection of specific information when it is obligated by law / regulations.
- When developing products or services, consider cybersecurity measures from planning / designing stage based on the concept of Security by Design.

Direction 5 Establish systems to effectively address cybersecurity risks

Establish a system to implement protection measures (measures for protection, detection and analysis) in order to address cybersecurity risks.

Scenario in case of no action for security

- If appropriate measures are not implemented against cybersecurity risks, damage may spread when a cyber-attack occurs.
- Without proper operation of the deployed measures for detection, analysis and response, it is impossible to grasp the overview of the cyberattack and it could cause severe damage such as theft of critical information of the organization.

Examples of recommended actions

- Implement multi-layer defense (defense-in-depth) for devices, networks, systems and services (including cloud services) on which important workload is conducted.
  -- Segregate network segments as necessary by switches or firewalls and operate them under different policies.
  -- Perform a vulnerability diagnosis etc. to detect system vulnerabilities and fix them.
  -- Implement data security measures, such as encryption, backup and unauthorized change monitoring, for sensitive information (trade secrets, highly confidential technical information, personal information etc.).
- Establish a system to monitor and detect cyber-attacks from access logs and network logs.
  -- Identify events that should be detected, and develop a system to detect those events and to take appropriate actions such as alerting security staff.
  -- As security monitoring requires professional skills, consider the use of external monitoring services if there are no professional human resources within the company.
- Be prepared to take appropriate response to cyber-attacks by providing training for employees on a regular basis.
  -- Train employees to implement and operate security measures thoroughly, such as software update and anti-malware software as a basis of cybersecurity, and monitor their performance.
  -- Train employees to report if they receive a suspicious email, and if that happens, alert and tell all the employees not to open similar emails.

Direction 6　Implement a PDCA cycle for cybersecurity measures

Implement cybersecurity measures as a PDCA cycle in order to execute and improve plans. As part of the PDCA cycle, regularly report the status of measures to management and make improvements if a problem occurs. Disclose the status of measures to enhance the trust of stakeholders.

Scenario in case of no action for security

- Without a structure that enables PDCA (Plan, Do, Check, and Act), there is risk that a plan might not be surely executed.
- It is also important to review cybersecurity measures on a regular basis from the perspective of whether the company is able to address the latest threats. Failure in these efforts might lead to the inability to cope with changes in the cybersecurity environment and risk of being unable to respond to newly emerging threats.
- Without proper disclosure of information on the status of measures, from the standpoint of social responsibility, trust from stakeholders with respect to cybersecurity might be lost and it might cause corporate value to fall greatly if an incident occurs.

Examples of recommended actions

- Develop a structure or process to continuously respond to cybersecurity risks (develop a PDCA cycle).
- Refer to Appendix A for the Check part of the PDCA cycle.
- Make use of international certifications such as ISMS as necessary.
- Set KPIs with respect to cybersecurity risk management and report the status to management at a committee related to corporate risks in the organization. Examples of KPIs include the number of items pointed out in risk analysis, ratio of people who have received security education within the organization, and number of incidents that occurred.
- Detect and resolve any issues regarding the current system and cybersecurity measures based on the results of security diagnoses and audits as necessary.
- Promptly modify the policy as needed when a new cybersecurity risk is identified.
- Consider incorporating the report on the status of cybersecurity measures into other reports such as the information security report, CSR report, sustainability report, and securities report in accordance with the nature or degree of cybersecurity risks.

3. 3. Establish a system to prepare for the occurrence of incidents

Direction 7　Develop a cybersecurity incident response team and relevant procedures

Establish a response structure within the organization (CSIRT, etc.) to identify the scope of impact and damage, take initial action in order to prevent further damage, and implement measures to prevent similar incidents from happening. Decide what information should be reported to whom in case of emergency, and support management to report that information to internal and external stakeholders appropriately.

Scenario in case of no action for security

- Without a system or structure for incident response, there will be difficulty communicating with internal and external stakeholders and quickly responding to the incident.
- Without prompt information disclosure, there is risk of damage spreading to customers and business partners and consequetnly the possibility of being liable for their damage.
- If reporting to relevant government agencies about the incidents that happened is mandatory by law and it's failed, there will possibly be legal penalty.
- Employees who have never received training or education about cybersecurity are not able to act appropriately when an unforeseen incident actually happens.

Examples of recommended actions

- Build a structure to do the following for the preparation of emergency.
  -- Conserve evidence such as various logs and devices infected with malware after being victimized by a cyber-attack for swift identification and analysis of the cause of damage, giving directions to employees to cooperate with relevant organizations for joint investigation. Moreover, in investigating the cause of an incident, it is recommended to also refer to Appendix C, "Items to organize within the organization for the occurrence of incidents."
  -- Execute drills in preparation for cyber-attacks including developing measures to prevent similar incidents from recurring and reporting to relevant government agencies. Consider consulting external experts as necessary for measures to prevent recurrence.
  -- Prepare a list of emergency contacts (security vendors etc.) and a list of organizations to disclose information to, including external parties, and share those

lists with incident response members.

-- Calculate the impact of first response on regular business operation and based on that, make arrangements in advance with other divisions of the organization (HR, sales etc.) for emergency.

-- Check relevant law / regulations and procedures to fulfill obligations described in the law / regulations.

-- Report to management the status of damage and impact to other companies due to the incidents.

Direction 8 Develop a recovery team and relevant procedures in preparation for damage due to cyber incidents

If business operations are suspended due to an incident, set recovery goal (by when operations should recover), taking into consideration the impact on corporate management, make a recovery procedure manual and develop a structure for recovery.
The recovery goal and plan should be consistent with organization-wide plans such as BCP. Additionally, execute practical drills to prepare for recovery from the suspension of operations.

Scenario in case of no action

- Essential operations cannot recover within an appropriate period and it causes a critical impact on corporate management.
- Without practical drills, personnel may not be able to act appropriately in unforeseen situations.

Examples of recommended actions

- Establish a recovery structure to implement the following in case of operation suspension.
  -- Give employees directions to do recovery tasks in cooperation with relevant organizations for prompt recovery in case of a cyber-attack. Additionally, personnel related to response should receive drills of the recovery procedures.
  -- Align the recovery goal (by when essential operations should recover) with an organizational plans such as BCP.

*Direction 7 and 8 mention drills of incident response and of recovery respectively. It is recommended to consider whether to execute them separately or together based on the contents of the drills and roles of the relevant parties of the organization.

3. 4. Drive security measures in the supply chain

Direction 9　Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies

A PDCA cycle of cybersecurity measures including auditing etc. should cover group companies, business partners and outsourcing companies in the company's supply chain.
When considering outsourcing operations such as systems management, the boundary between insourcing and outsourcing should be set appropriately.

Scenario in case of no action

- If there are vulnerable point in the supply chain, the company might be attacked via those weak partners, and possibly, the company could cause collateral damage to other companies. Additionally, as it's often difficult for those vulnerable partners to cooperate in incident response (collect logs etc.), incident response process will be difficult and as a result, it could cause impact on business operation.
- When outsourcing tasks such as system management, unclear segmentation of insourcing and outsourcing could cause oversight of tasks.

Examples of recommended actions

- Make a contract after clearly understanding measures deployed in the partner.
- Receive reports on the status of cybersecurity measures (including audits) from the partners.
- When entrusting outsourcing companies with sensitive information such as personal information or technical intelligence property, conduct periodical check whether or not the entrusted information is secured in the partner's environment, taking into account the business situation of the partner.
- Confirm the partner takes part in the SECURITY ACTION program.[9] Additionally, it is desirable if they have acquired security management certification such as ISMS.
- In preparation for costs that will be needed if incident ocurrs in the partner, it is desirable if they have purchased cyber insurance.

9. A program for small and medium-sized companies to declare their commitment to security measures
https://www.ipa.go.jp/security/security-action/

3. 5. Drive communication with stakeholders and other relevant parties

Direction 10 Gather, utilize, and provide cyber-threat information through information sharing activities

In order for the whole society to have capability against latest cyber-attacks, participate in information sharing activities on cyber-attacks.
Additionally, develop environments to effectively utilize the information obtained.

Scenario in case of no action for security

- If information on a specific cyber-attack is not shared among companies, each company needs to fight against the same cyber-attack individually and it will increase cybersecurity cost in each company.

Examples of recommended actions

- It is needed to protect the whole society, not company by company, from cyber-attacks through mutual information sharing among organizations. In order to do that, actively providing information for others is essential, as well as taking information from others.
- Make the best use of security alerts, such as vulnerability information, from IPA, JPCERT Coordination Center (JPCERT/CC, general incorporated association) etc..
- Make the best use of information obtained through private activities of information sharing among CSIRTs (Computer Security Incident Response Team) and through communities hosted by the Nippon CSIRT Association.
- Report information on malware and unauthorized access to the IPA based on the regulations (Computer Virus Countermeasures Standard and Unauthorized Computer Access Countermeasures Standard).
- Provide information on incidents for the JPCERT/CC and request coordination if needed.
- Critical infrastructure operators should also consider joining J-CSIP.

Appendix A: Check sheet of cybersecuriy management

*This check sheet lists only basic items for cybersecurity management and the implementation of additional measures is important according to the situation of each company.

*The check sheet items and corresponding relationship with the NIST Cybersecurity Framework [10] will be displayed. (The information in the parentheses corresponds to the subcategory identifiers in the NIST Cybersecurity Framework.)

Direction 1: Recognize cybersecurity risk and develop a company-wide policy

☐	Management recognizes cybersecurity risk as part of management risk.	(－)
☐	Management has developed and published a company-wide security policy taking cybersecurity risks of the company into consideration.	(ID.GV-1)
☐	Management understands requirements in law / regulations and industry-specific guidelines.	(ID-GV-3) (DE.DP-2)

Direction 2: Build a management system for cybersecurity risk

☐	A structure for cybersecurity risk management consisting of a CISO, etc. has been established based on the company's security policy.	(－)
☐	The role and responsibility of each relevant person in the cybersecurity risk management structure is defined.	(ID.GV-2)
☐	The relationship between the corporate risk management structure and the cybersecurity risk management structure within the organization is defined.	(ID-GV-4)

Direction 3: Secure resources (budget, workforce etc.) for cybersecurity measures

☐	Cybersecurity measures needed for the organization are identified, budget for them has been approved in corporate management-level meetings, and the budget is actually secured.	(－)
☐	Human resources for cybersecurity are secured and each person (both internally and externally) understands their role.	(PR.AT-2) (PR.AT-3) (PR.AT-4) (PR.AT-5)
☐	Cybersecurity talents are developed and trained within the organization.	(PR.AT-1)
☐	Career paths inside the company are designed for cybersecurity resources, and they are properly treated.	(－)
☐	Trainings on security are provided on a regular basis for all the employees, not only for security staff.	(PR.AT-1)

[10] Framework for Improving Critical Infrastructure Cybersecurity (NIST)
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Direction 4: Identify cybersecurity risks and develop plans to address them

☐ Information to be protected is identified and prioritized based on its storage location, value for business etc..	(ID.AM-1) (ID.AM-2) (ID.AM-3) (ID.AM-4) (ID.AM-5)
☐ Cyber threats to and vulnerabilities of the specified information to be protected are identified and recognized as cybersecurity risks based on corporate strategy.	(ID.RA-3) (ID.RA-1) (ID.RM-1)
☐ How cybersecurity risks affects the business is anticipated.	(ID.RA-4) (ID.RA-5) (ID.RM-2)
☐ A risk management plan is developed to avoid / mitigate / transfer cybersecurity risks in accordance with the degree of impact of each risk.	(ID.RA-6) (ID.RM-3)
☐ Cybersecurity risks which don't require actions to be taken because of their impact level are identified and recognized as residual risks.	(ID.RA-6) (ID.RM-3)

Direction 5: Establish systems to effectively address cybersecurity risks

☐ Multi-layer defense such as the separation of network segments, access control, and encryption is implemented on devices, networks, systems, and services on which important operations are conducted.	(PR.AC) (PR.DS)
☐ Vulnerability diagnoses are performed, and actions are taken to vulnerabilities detected.	(PR.IP-12)
☐ Events that should be detected (for example unauthorized access) are specified and measures to promptly detect such events are in place, including systems, procedures such as log collection and analysis and structures.	(DE.AE-1) (DE.AE-5) (DE.DP-3)
☐ A response plan has been developed for when events are detected. (impact of each type of event, responsibility assignment of responders etc.)	(DE.AE-4) (DE.DP-1) (DE.DP-4)
☐ The cybersecurity measures (list of events that should be detected, enhancement of technical measures etc.) are reviewed and updated accordingly based on cyber-attack trends etc.	(DE.DP-5)
☐ Employees are provided with education on cybersecurity, ranging from raising awareness for basic cybersecurity actions such as software update, anti-malware software usage to training against targeted attack emails..	(PR.AT-1)

Direction 6: Implement a PDCA cycle for cybersecurity measures

☐	Management receives regular reports on the status of cybersecurity measures and understand it.	(—)
☐	External audits are conducted for cybersecurity.	(—)
☐	Cybersecurity risks and threats are reviewed as necessary, and the structure for cybersecurity (PDCA) is maintained accordingly.	(PR.IP-7)
☐	Cybersecurity risks and activities of the company against those risks are disclosed to external stakeholders.	(—)

Direction 7: Develop a cybersecurity incident response team and relevant procedures

☐	Internal and external emergency contacts and communication routes are listed and maintained (such as system operators, website maintainers/ operators and contracted security vendors).	(RS.CO-3) (RS.CO-4) (RS.CO-5)
☐	An initial response manual against cyber-attacks has been developed and maintained.	(PR.IP-9) (RS.RP-1)
☐	A dedicated team for incident response (CSIRT etc.) has been established and maintained.	(RS.CO-1)
☐	Rules to report management have been established (reporting lines, timing, which information to disclose etc.) so that management can properly explain about the incident to both internal and external stakeholders.	(RS.CO-2)
☐	The initial response manual is reviewed and updated taking into account issues found in the past incident response.	(RS.IM-1) (RS.IM-2)
☐	Response drills and exercises are performed on a regular basis, which include the development of post-incident recurrence prevention measures.	(PR.IP-10)

Direction 8: Develop a recovery team and relevant procedures in preparation for damage due to cyber incidents

☐	A recovery plan for operations has been developed in preparation for damages from incidents.	(ID.BE-5) (PR.IP-9) (RC.RP-1)
☐	The recovery plan is reviewed and updated according to issues found in past recovery activities.	(RC.IM-1) (RC.IM-2)
☐	Internal and external emergency contacts and communication routes are listed and maintained.	(RC.CO-1) (RC.CO-2) (RC.CO-3)
☐	Recovery drills and exercises are performed on a regular basis.	(PR.IP-10)

Direction 9: Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies

☐	Insourcing and outsourcing are appropriately separated based on the company's in-house resource and importance of each function to the company.	(ID.BE-3) (ID.BE-4)
☐	Cybersecurity measures which outsourcing partners should implement in themselves are clearly stipulated in contracts etc.	(ID.AM-6) (ID.BE-1) (PR.IP-8)
☐	Cybersecurity status, including audit results, of partners (group companies, outsourcing companies, business partners in supply chain etc.) are regularly reported and understood.	(—)

Direction 10: Gather, utilize, and provide cyber-threat information through information sharing activities

☐	Cybersecurity information are obtained and utilized for the company's actions by monitoring security alerts from industrial organizations or joining communities for information sharing.	(ID.RA-2)
☐	When the company acquired information on malware or unauthorized access or experienced incidents, it shares that information with the information sharing activities operated by various organizations such as IPA, JPCERT/CC, security vendors etc.	(ID.RA-2)

Appendix B: Reference information on cybersecurity

Information that will serve as reference for information systems departments in charge of cybersecurity measures in implementing the ten important items in these Guidelines are given below. The published URL for each guideline will also be provided, but because the guidelines may be updated, it is recommended to refer to the latest version as necessary.

Reference material related to the ten important items in general

- Manual for the Cybersecurity Management Guidelines [Ver.1.0] (IPA)

  (A manual to explain the concept on how to concretely implement the three principles and ten important items of the Cybersecurity Management Guidelines)

  - https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html

- Information Security Measure Guidelines for Small and Medium-sized Enterprises [Ver. 2.1] (IPA)

  (Guidelines explaining points for small and medium-sized enterprises to undertake security measures. It includes appendices such as the Five Articles of Information Security which lay out the measures that are needed at the minimum and the Five-Minute Information Security Self-Diagnosis.)

  - https://www.ipa.go.jp/security/keihatsu/sme/guideline/

- ISO/IEC 27002:2013（ISO/IEC）

  (The international standard which sets the specifications for information management systems. It provides the best practices in information security management.)

- Framework for Improving Critical Infrastructure Cybersecurity [Version 1.0] (NIST)

  (US guidelines dividing cybersecurity measures that companies involved with critical infrastructure should implement into the five functions of "identify," "protect," "detect," "respond," and "recover," the functions of which are further divided into 22 categories. They can be utilized by companies other than those engaged with critical infrastructure as well.)

  - https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

- SP800-53 [Rev. 4] (NIST)

  (US guidelines stating security measures that federal agencies should implement. When providing cloud services to the US federal government, compliance with these guidelines may be required.)

  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- SP800-171 [Rev. 1] (NIST)

  (US guidelines stating security measures that should be implemented by organizations other than federal agencies and to protect CUI.[11] When being contracted to do work for the US federal government, compliance with these guidelines may be required.)

  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

11 An abbreviation for Controlled Unclassified Information. CUI indicates important information that should be controlled, but for which the federal government has not prescribed special classifications such as secret, top secret, or confidential.

Reference material related to Direction 3

- Guide for developing human resources in charge of information security with the use of IT skill index [May 2015] (IPA)

  (Guidelines illustrating what kind of measures are necessary to prevent cyber-attacks, what kind of human resources are necessary to implement such measures, and summarizing tips for training human resources.)

  https://www.ipa.go.jp/files/000039528.pdf

- Skill-Up Guide for Information Security Administrators at the Workplace [September 2015] (IPA)

  (Guidelines illustrating what kind of measures should be implemented for security threats and preventing damage, and indicating the specific role of security administrators.)

  https://www.ipa.go.jp/files/000047872.pdf

Reference material related to Direction 4

- Information Security Measure Guidelines for Small and Medium-sized Enterprises [Ver. 2.1] (IPA)

  (Explains the risk analysis method in Chapter 4 of these Guidelines. Additionally, they present a risk analysis sheet to support the implementation of risk analysis as an appendix.)

  https://www.ipa.go.jp/security/keihatsu/sme/guideline/

Reference material related to Direction 5

- System design guide for responding to 'advanced targeted attack' [September 2014] (IPA)

  (Guidelines explaining internal measures taken against targeted attacks aimed at preventing the spread of damage and enhancing monitoring, premised on system infiltration.)

  https://www.ipa.go.jp/security/keihatsu/sme/guideline/

- Use and method of analysis of log in relation to response against advanced cyber attack [Ver. 1.0] (JPCERT/CC)

  (Guidelines describing the idea of leaving the traces of attackers' activity on typical equipment as a log and how to find traces from such logs, from the viewpoint of preparation against cyber-attacks and effective measures.)

  https://www.jpcert.or.jp/research/apt-loganalysis.html

- Guidelines for the Prevention of Internal Improprieties in Organizations [Ver. 4] (IPA)

  (Guidelines that present 30 measures based on 10 points (compliance, workplace environment, etc.) to take in order to prevent internal improprieties in organizations.)

  https://www.ipa.go.jp/files/000057060.pdf

- Handbook for Protecting Confidential Information [February 2016] (Ministry of Economy, Trade and Industry)

  (A handbook that introduces a collection of examples of measures to prevent the leakage of confidential information.)

  http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

Reference material related to Direction 6

- Information Security Management System (ISMS) Conformity Assessment Scheme (JIPDEC)

  (A scheme for third-party certification for information security management systems based on international standard ISO/IEC27001.)

  https://isms.jp/isms.html

- Cyber Security Management System (CSMS) Conformity Assessment Scheme (JIPDEC)

  (A scheme for third-party certification for cyber security management systems based on international standard IEC62443-2 targeting industrial automation and control systems.)

  https://isms.jp/csms.html

- Information Security Management Standards (Ministry of Economy, Trade and Industry)

  (Comprehensive standards covering the establishment of information security management to concrete management measures that are consistent with international standard ISO/IEC27001.)

  http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html

- Information Security Measures Benchmark (IPA)

  (A tool to display a company's status of implementation of security measures as a scatter diagram, radar chart, scores, etc., by answering questions online. It also allows companies to compare their status of measures with that of other companies.)

  http://www.ipa.go.jp/security/benchmark/

- How to Secure Your Web Site [Ver. 7] (IPA)

  (Guidelines presenting technical measures to create a website that takes security into account. A supplementary volume also provides online health diagnosis specifications presenting test items to check a website for vulnerabilities.)

  https://www.ipa.go.jp/security/vuln/websecurity.html

- JVN (IPA, JPCERT/CC)

  (A portal site for measures against vulnerabilities, which provides information on vulnerabilities in software used in Japan and their countermeasures.)

  https://jvn.jp/

Reference material related to Direction 7

- CSIRT Establishment Materials (JPCERT/CC)

  (Guidelines explaining points to take into account at the "initiative phase," "establishment phase," and "operation phase" respectively for establishing a CSIRT in order to conduct systematic incident response.)

  https://www.jpcert.or.jp/csirt_material/

- Reference materials useful for establishing a CSIRT (Nippon CSIRT Association)
  (A collection of reference material gathering documents for each stage of establishing a CSIRT, from beginners, for when explaining for management, and planning, establishing, and operating by personnel in charge of establishment.)

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

Reference material related to Direction 8

- Business Continuity Guidelines [revised August 2013] (Cabinet Office)
  (Guidelines which clarify the necessity of business continuity and present items for which implementation is necessary and items for which implementation is recommended for the development and revision of a business continuity plan.)

  http://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline03.pdf

Reference material related to Direction 9

- Guidelines on the promotion of the improvement of subcontracting transactions in information service/software industry [March 2017] (Ministry of Economy, Trade and Industry)
  (Guidelines developed for the purpose of promoting fair subcontracting transactions, which explains items to take into account for efforts related to personal information protection and security measures.)

  http://www.chusho.meti.go.jp/keiei/torihiki/2014/140313shitaukeGL3.pdf
- SECURITY ACTION (IPA)
  (A program for small and medium-sized companies to declare their commitment to security measures.)

  https://www.ipa.go.jp/security/security-action/

Reference material related to Direction 10

- Report, Consult, and Share Information (Report Unauthorized Access, Viruses, Etc.) (IPA)
  A website that provides report templates, report contacts, and report statuses for reports on computer viruses, unauthorized access, and vulnerabilities.)

  https://www.ipa.go.jp/security/outline/todoke-top-j.html
- Special help desk for targeted cyber-attacks (IPA)
  (A consultation desk for expert counselors to consult after receiving a targeted cyber-attack.)

  https://www.ipa.go.jp/security/tokubetsu/
- Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) (IPA)
  (An initiative to share information and conduct early response in critical infrastructure equipment

manufacturing, electricity, gas, chemical, oil, resource development, automotive, and credit industries.)

https://www.ipa.go.jp/security/J-CSIP/

- @police (National Police Agency)

  A website that provides various information related to network security, in order to prevent cybercrimes and cyber terrorism as well as prevent damage from cybercrimes and cyber terrorism from spreading.)

  https://www.npa.go.jp/cyberpolice/

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

Ten important items	ISO/IEC 27001 (●), ISO/IEC 27002 (-)	
Direction 1 Recognize cybersecurity risk and develop a company-wide policy	● 5.1	Leadership and commitment
	● 5.2	Policy
Direction 2 Build a management system for cybersecurity risk	● 5.3	Risks and opportunities, responsibilities and authorities
	- 6.1.1	Information security roles and responsibilities
Direction 3 Secure resources (budget, workforce etc.) for cybersecurity measures	● 7.1	Resources
	● 7.2	Competence
Direction 4 Identify cybersecurity risks and develop plans to address them	● 6.1	Actions to address risks and opportunities
	● 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
Direction 5 Establish systems to effectively address cybersecurity risks	- 6.2	Mobile devices and teleworking
	- 9	Access control
	- 10	Cryptography
	- 11	Physical and environmental security
	- 12	Operations security
	- 13	Communications security
Direction 6 Implement a PDCA cycle for cybersecurity measures	● 7.4	Communication
	● 8.1	Operational planning and control
	● 8.2	Information security risk assessment
	● 8.3	Information security risk treatment
	● 9.1	Monitoring, measurement, analysis and evaluation
	● 9.2	Internal audit
	● 9.3	Management review
	● 10.1	Nonconformity and corrective action
	● 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
Direction 7 Develop a cybersecurity incident response team and relevant procedures	- 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
Direction 8 Develop a recovery team in preparation for damage due to cyber incidents	- 17.1.1	Planning information security continuity
	- 17.1.2	Implementing information security continuity
	- 17.1.3	Verify, review and evaluate information security continuity
Direction 9 Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies	● 8.1	Operational planning and control
	- 15.1.1	Information security policy for supplier relationships
	- 15.1.2	Addressing security within supplier agreements
	- 15.1.3	Information and communication technology supply chain
	- 15.2.1	Control and review of supplier services
	- 15.2.2	Managing changes to supplier services
Direction 10 Gather, utilize, and provide cyber-threat information through information sharing activities	- 16.1.3	Contact with authorities
	- 16.1.4	Contact with special interest groups

Appendix E: 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

Cybersecurity is an effort to prevent information leaks or IT system malfunctions which occur due to cyber-attacks.

5) Cybersecurity risk

Cybersecurity risk is probability of negative impact on business management resulting from occurrence of cybersecurity-related problems.

6) Residual risk

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

7) Information security report

A report which discloses a company's efforts for information management and information security, 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

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 malware 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 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 "effect of uncertainty on objectives."

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

Ways to respond to risk largely include four responses of "risk avoidance," "risk reduction," "risk

transfer" and "risk acceptance." According to JISQ0073 Risk Management -Vocabulary, these risk responses are categorized into seven elements such as risk avoidance, risk taking or increasing to gain opportunity, elimination of risk reduction, alternation of risk likelihood, change of result, risk transfer, risk acceptance.

(1) Risk avoidance

"Risk avoidance" 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 unauthorized access from the internet."

(2) 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 unauthorized access, and providing training on information security for personnel.

(3) 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 unauthorized access or malware infection based on these contracts.

(4) 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 of use of computers or data transmission. 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) BCP (Business Continuity Plan)

A plan that sets out methods for business continuity in normal time and in emergencies for the continuity of the core business of a company and realize early recovery when it incurs damage due to a natural disaster, terror attack, cyber-attack, etc.

19) CISO (Chief Information Security Officer)

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

20) CSIRT (Computer Security Incident Response Team)

Structure to respond in the occurrence of an incident.

21) 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.