

Chief Information
Security Officer

Guidebook

Basic



Ministry of Science and ICT

<https://t.me/learningnets>



Korea Internet &
Security Agency

CSO Guidebook

Basic

This guidebook has been published by compiling the materials used in the Basic Course of the Capacity Building Education for Chief Information Security Officers (CISOs) conducted in 2019. This book may contain the private opinions of the authors.

About the Authors



Kang Eun-Seong

Representative Kang Eun-Seong is one of Korea's best security experts who served as the research director of the largest security company in Korea and the chief security officer (CSO) of an Internet portal company.

He established CISO Lab, providing consulting services and education on personal information protection and information protection. He authored IT Security (Hanul, 2009) and Information Security That the CxO Should Know (Hanbit Media, 2015).

(present) Professor of Department of Cyber Security of Ewha Womans University

(present) Representative of CISO Lab

(former) CISO/CPO of Blockchain OS



Hong Sung-kwon

Technical Expert Hong Sung-kwon is providing companies with consulting services related to the establishment of personal information and information protection system, OT security, global compliance (General Data Protection Regulation (GDPR)), etc. and teaching at the Korea CPO Forum, National Human Resources Development Institute, business entities, etc.

(present) Director of Consulting Division in Norma

(present) Technical Expert at Law Firm Lin

(former) CS/Director in Advisory HQ of EY Korea

Qualification certificates: ISMS-P Examiner, ISO27001 Auditor

E-mail: sungkwon.hong@gmail.com



Baek Je-Hyeon LL.D.

(present) Adjunct Professor at Dept. of Scientific Investigation of Sungkyunkwan University

(present) CISO, MESHKOREA Co., Ltd

(present) Representative of Security InSight LAB

(present) Regular member of Korea ISLA Winners' Association (KISLAA)

(former) (IVice Chairperson of SC)² KOREA Chapter d

(former) CISO of With Innovation Co., Ltd.

(former) (ISC)² CISSP Authorized Instructor

2012 Won Asia-Pacific ISLA award

CISSP | CISA | CCFP | EnCE

I	What is CISO?	
	1. Introduction - Victory of Defence	8
	2. Corporate Management and Information Protection	10
	3. Information Protection Work and Information Protection	14
	4. The Duty of CISO	23
	5. Conclusion	35
II	CISO's Awareness	
	1. The Laws that CISO should know	39
	2. The Security that CISO should know	58
III	The Establishment of Information Protection Regulations	
	1. Overview of Information Protection Regulations	65
	2. How to Prepare Information Protection Regulations	68
	3. Cases of Information Protection Regulations	71
IV	Raising Awareness of Employees	
	1. Prologue	80
	2. Information Protection ... Why is it Important?	87
	3. Measures to Raise Awareness of Information Protection; understanding the basic concept and steps	95
	4. Measures to Raise Awareness of Information Protection; Step by step and specific measures	101
	5. Information Security Education Plan; To Remind Employees of Information Security	118
	6. Security Culture Settlement Plan; Quantification of Security Indicators	126
	7. Epilogue	133



the CISO

Guidebook

Basic



What is CISO?



1. Introduction – Victory of Defence
2. Corporate Management and Information Protection
3. Information Protection Work and Information Protection Governance
4. The Duty of CISO
5. Conclusion

1. Introduction - Victory of defence



Lionel Messi of Argentina playing against Croatian players in a Group-D match of 2018 FIFA World Cup held in Russia: In the match, Argentina was completely defeated by Croatia by the score of nothing to three. (OhmyNews, June 22, 2018)

Lionel Messi is acknowledged to be the best striker in the world. The fact that he has received the Ballon d'Or, which is generally regarded as the most prestigious individual award for football players, three times proves that he is really an amazing player. Nonetheless, Messi has never won a competition among national teams such as the FIFA World Cup as soccer is not a sport that can be played well by only one star player. In particular, the Argentine team often lost a game by a large margin due to poor defense. For example, in the 2018 FIFA World Cup Russia, the Argentine team lost to Croatia 0-3 and to France 3-4. As a result, Argentina was eliminated in the first round at the 2018 World Cup.

While the 2018 FIFA World Cup Russia was a nightmare for Argentina, it stays with the Korean people as a happy memory because the Korean team defeated the German team, which had been the champion team of the 2014 FIFA World Cup Brazil and was ranked No. 1 at that time, with the final score of two to nothing. Though Korea was not able to advance to the round of 16, the victory of Korea against Germany -- the strongest team in the world -- was a shock not only to the Korean people but also to all soccer fans around the world as Germany was eliminated in the preliminary round of the World Cup due to that defeat.



Korea beat Germany 2-0 in a Group-F match of 2018 FIFA World Cup Russia. Hyun-Woo Cho, goal keeper of the Korean team, was named the Man of the Match by his excellent defense in the match. (The Fact, June 27, 2018)

In a word, Korea's victory against Germany was achieved by good defense. In the match, the Korean national team stopped the offense of the world's best team - Germany -- by using the ultimate measure of "Everyone defends," with Korean goalkeeper Hyun-Woo Cho denying many shots that could have scored goals and consequently getting named Man of the Match for his excellent play. The match showed well how important defense is, and the game stood in stark contrast to the play of the Argentine team, which had the best striker in the world.

There are offense and defense in the area of business management, too. While the company's departments that work to achieve the business goals of the company such as sales, operating income, traffic, number of customers, etc. can be called the strikers of the company, the departments managing the risks that can occur in the process can be regarded as defenders. The organizations working for sales, marketing, and product or service development and the supporting IT operation department may be called strikers, whereas the departments managing various kinds of risks including legal risk, financial risk, mass media risk, personnel management risk, security risk, and personal information leak risk, etc. may be called the defenders.

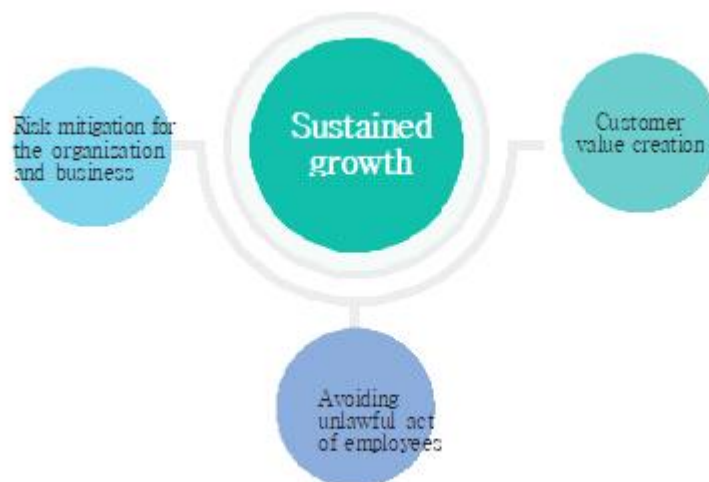
While the strikers of a company are the departments that focus on the short-term growth of the company, the defenders are the departments providing support for the mid- and long-term solid growth and development of the company by managing its risks. Many companies were severely hit by the foreign exchange crisis in 1997 and the global financial crisis in 2008 while focusing on short-term growth. Those cases speak volumes about the great importance of risk management in corporate management.

2. Corporate Management and Information Protection

(1) The purpose of Information Protection

Traditionally, it has been explained that the purpose of Information Protection is to protect the Confidentiality, Integrity, and Availability of information assets. Although technically right, it does not explain the contribution made by Information Protection to corporate management, and it shows that Information Protection remains in the realm of technology and technical experts. A company's chief information security officer (CISO) is supposed to explain the role and value of Information Protection to the top management. Of course, it is necessary to explain Information Protection in the aspect of corporate management.

Figure 1-1 The purpose of Information Protection in the aspect of corporate management



As mentioned in the previous page on the explanation of defenders of a company, the department in charge of Information Protection takes care of the security risk of the company. Security risk largely includes the risk inherent in the organization, business, and service and the risk concerning the executives and staff members. The mission of the Information Protection department is to manage and minimize both types of risk for the sustained growth of the company.

Information Protection can also create customer value. Excluding security products whose customer value is security, there were few cases wherein security was included in customer value. In Korea, the “Vega Secret Phone” of Pantech introduced a hidden function for user authentication in photo album, video, App, etc. with the fingerprint verification technology already in 2013 to provide the value of protection of customers' privacy. Apple's iPhone was the first to offer full-scale, safe, and convenient customer value with security by using fingerprint verification technology for user authentication for mobile phone itself and financial transaction.

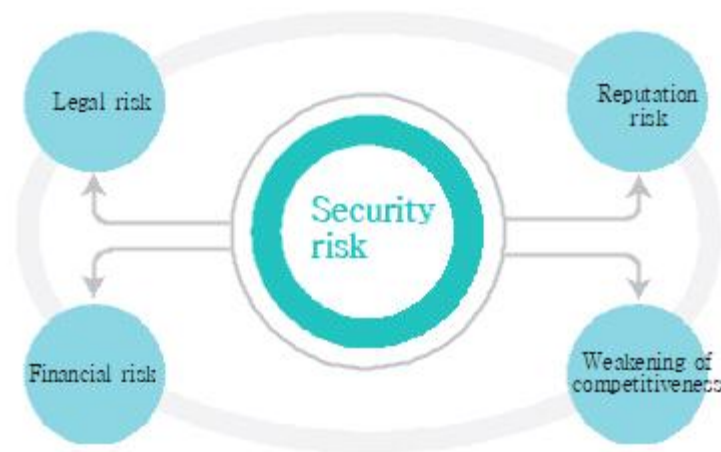
Figure 1-2 Example of corporate level risks



(2) Corporate-level security risk

Upon setting a business goal or a managerial objective, a company implements it by constantly managing related risks. There are international standards and classification methods for corporate risks. <Figure 1-2> shows an example of the risks that must be managed at the corporate level in ordinary companies. Legal risk and financial risk used to be objects of conventional risk management, and reputation risk has become a big issue recently. If a problem arises with reputation, the general opinion of the society will be inflamed, and an investigation by the authorities can begin to expand it to a legal problem and even cause financial risk due to a boycott campaign or the imposition of penalty surcharge. With respect to disaster risk, while there are many natural disasters, there are also social disasters even though they do not occur frequently, and there is an organization or a business to inspect carefully.

Figure 1-3 Security risk as a corporate level risk

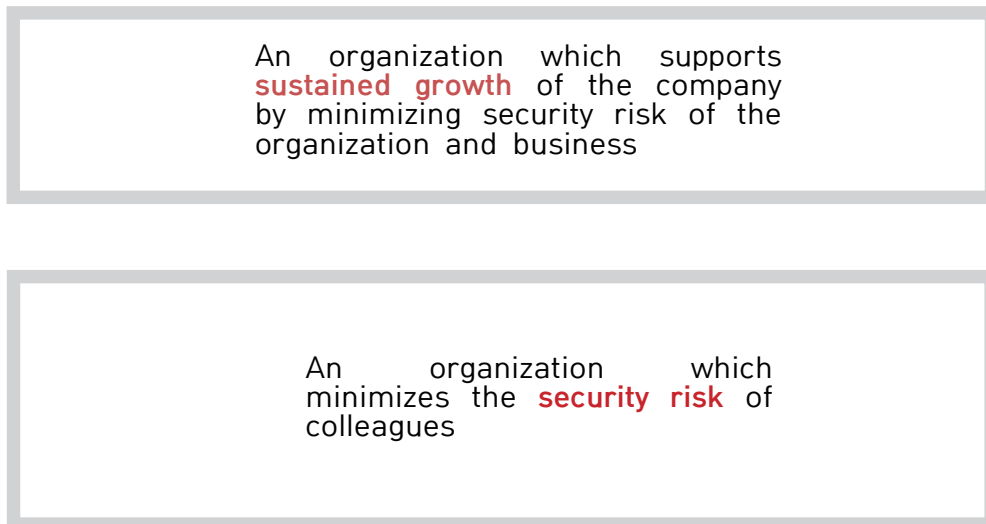


The area of security is strictly regulated. Many offline companies are using the Internet for their business, and such companies are regulated by the Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (hereinafter referred to as “Information and Communications Network Act”) and the Personal Information Protection Act in addition to the provisions on personal information protection in the Information and Communications Network Act if they collect and use the personal information of customers. If a company holds more than a certain level of personal information, or sales are generated in the IT service sector, the company is required to obtain certification for Information Protection and personal information protection management system. A legal risk occurs if the relevant laws and regulations are not observed, whereas a reputation risk arises if the problem with security or personal information protection issue is revealed to the public. A financial risk occurs if a penalty is imposed or a civil lawsuit is filed. A management risk can be caused by various factors including market competition, cash flow, technological weakening, excessive M&D, etc., but security risk has certainly emerged as one of the causes of management risk.

(3) The role of CISO's organization

In this regard, it will be appropriate to define the mission of the Information Protection department as follows in the aspect of corporate management and business:

Figure 1-4 Mission of Information Protection department



The mission of the CISO can also be defined as follows in the aspect of corporate management and business.

Figure 1-5 Mission of CISO



3. Information Protection Work and Information Protection Governance

(1) Information Protection work vs. Information Protection Department's work

Usually, work carried out by the CISO and the Information Protection department is called Information Protection work. Still, not all the Information Protection works needed to be done in the company are carried out by the CISO's organization. It is similar to the case of personnel evaluation, which is run by the Personnel Department but is actually decided by the head of each department or executives. The Personnel Department prepares the standards, methods, and procedures for personnel evaluation, provides support if any problem occurs in the process of personnel evaluation, and, if necessary, offers the personnel evaluation materials of the heads of the major departments of the company for reference of the management.

Figure 1-6 Information Protection work and Information Protection department

Categories	Information Protection department	Non-Information Protection department
Information protection work	Information Protection management system, security technology, and responding to security issues	Outsourcing security, New employees and retirees security, IT infra operation security
Non-Information Protection work	Personnel management, General affairs	Sales, Marketing, Development, IT operation, Personnel management, General affairs

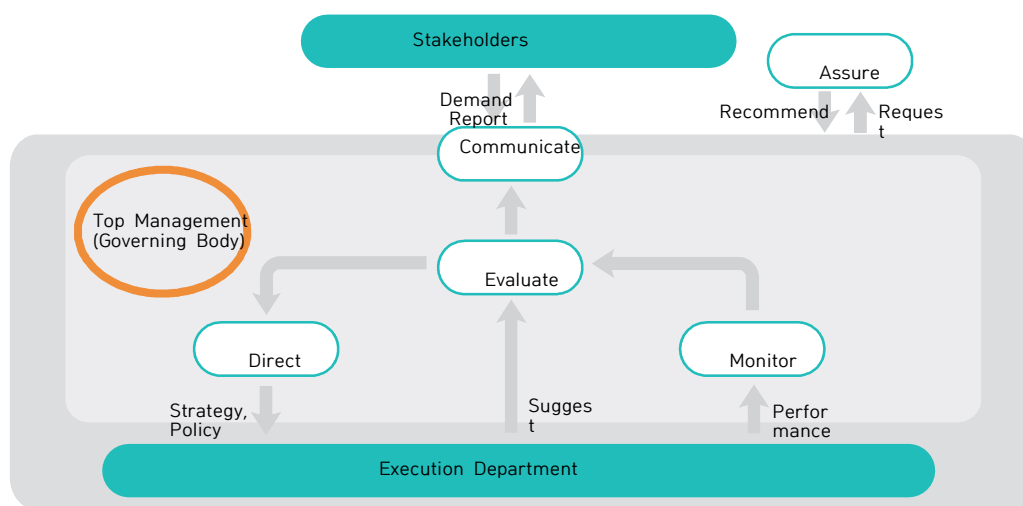
Likewise, Information Protection work, too, is being carried out by the Information Protection department and other departments as well. For example, in <Figure 1-6>, the Information Protection department performs the establishment and operation of the Information Protection management system, responds to various security issues, and carries out operation and analysis of some security solutions, etc.; if the IT system of the company is being developed by outsourced services, however, the outsourcing management department or the IT operation department will be responsible for the preparation of security pledges of the outsourced workforce concerned, provision and collection of information assets like PCs, management of server accounts, etc. For a new employee, the security pledge is submitted to the Personnel Department, and security education is conducted by the Information Protection department. In other words, Information Protection work is a company-wide work performed by the collaboration between the Information Protection department and Non-Information Protection department. In addition, it should be noted that Information Protection personnel need to have communication and collaboration capacity in order for the Information Protection department to take the initiative in performing the company-wide work.

As we have reviewed so far, Information Protection risk is a corporate-level risk; thus, the work of management of Information Protection must be conducted and controlled by the top management throughout the company with great interest.

(2) Information Protection governance

Business entities already have a mechanism for managing various kinds of company-wide risks. When the UK first raised the issue of Brexit, companies that had business interest with EU or which were critically affected by exchange rates must have begun to assess the expected influence of Brexit on their businesses. Security risk can also be assessed with such mechanism.

Figure 1-7 Process of Information Protection governance



Information Protection governance is the structure of making managerial decisions on Information Protection based on corporate governance.

As the international standard for Information Protection governance, ISO 27014 defines the process of Information Protection governance process as shown in <Figure 1-7>. The following is the process related to it:

The Execution department, including the Information Protection department and the Non-Information Protection department, proposes (reports) the policy, project, organization, etc. related to Information Protection.

- ♦ The top management²¹ reviews and evaluates the contents of the report of the Execution department.
- ♦ If deemed necessary to implement the contents of the report, the top management directs the related strategy and policies to the Execution department

The top management observes and evaluates the performance of the execution department.

- ♦ The top management communicates the security task or the results of its performance with stakeholders.
- ♦ The top management requests an objective, professional agency to check whether the security measures are conducted well and review the results.
- ♦ The Execution department works through collaboration with other departments that perform communication with the top management and security work.

¹ A compound word of Britain and exit

You may ask, “Will the top management of the company be able to take the initiative in the process?” Note, however, that such question is in the same context as whether the top management has expertise in deciding a new large-scale business, securing a big client, investing in development, etc., which used to be regarded in general as the role of the top management. Sometimes, the top management may push ahead with a project with expertise in the relevant area, but in many cases just makes a managerial judgment based on the report and advice of good staff members. As shown in <Figure 1-7>, a security risk is also a matter decided by the top management in the area of risk management for the company with the report and advice of a good staff. In Korean corporate governance, the CISO is seldom included in the top management. Thus, the role of the top management in Information Protection governance is very important.

Figure 1-8 The role of thace top management in Information Protection

Compose and empow Information Protection department	Approve and support Information Protection program and investment	Communicate with company-wide departments and support collaboration
• (Executive level) Appoint and empower CISO • Organize Information Protection department and support work force	• Mitigate security risk of the company and business • Understand security risk related to managerial objective	• Support collaboration of Information Protection department and line organization • Regular company-wide communication about security risk

The top management is the final decision maker on the organization, work force, and budget matters. The same is true for the matter of Information Protection.

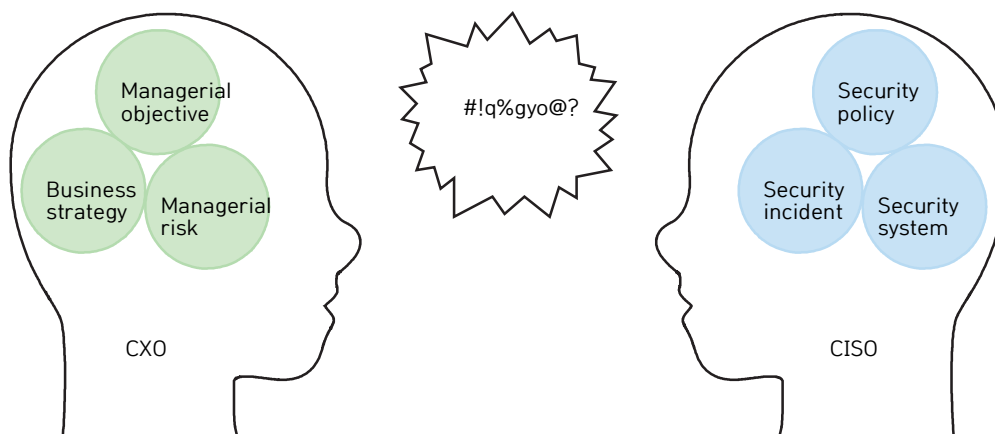
In particular, it is as important as anything else to appoint and empower an executive-level CISO who will manage the company-wide security risk as a member of the management because a company is a hierarchical organization wherein the persons are given authority and responsibility according to their duties and positions. Another important Information Protection work of the top management is to organize the department and provide workforce for the CISO's organization.

In addition, the top management must decide whether or not to approve the Information Protection program and investment and, in order to do so, grasp various managerial risks and security risks arising in the course of achieving the business goals. Moreover, the top management should play a certain role in the communication and collaboration between the Information Protection department and other departments as collaboration in a company can be promoted based on the firm will and company-wide communication of the top management in general. An important role of the CISO is to bring out such role of the top management.

(3) Communication with the top management

As in other areas, communication and collaboration in a company are affected by the capacity and efforts of individuals but are influenced much more by governance as well as the relationship between departments based on it, since a company is an organization that achieves its managerial objective by concentrating the power of all the departments of the company.

Figure 1-9 Communication with the top management



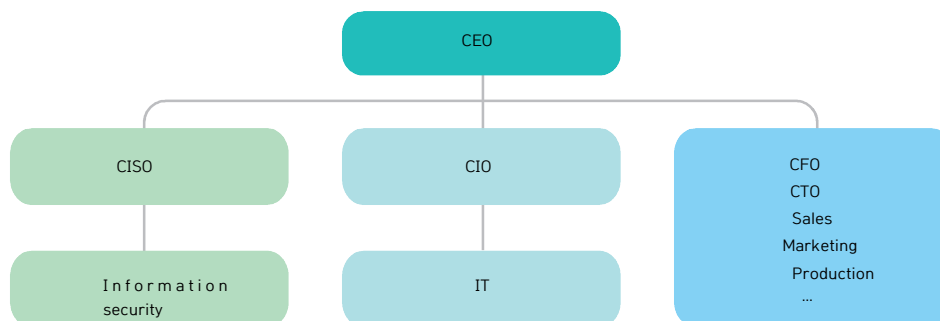
The CISO should try first to communicate with the top management. The major agenda of the top management includes managerial objective, business strategies to achieve the managerial objective, and related managerial risks. Managerial judgment on Information Protection is made in such frame, with the reports in the area of Information Protection often treated as technical issues. When introducing new company-wide security policy or security system, it will be difficult to have the top management understand it unless reported as an object of managerial judgment in relation to sales, operating profit, legal affairs, customer, traffic, etc.

In addition, though the CISO may deem every security issue to be important, there must be an order of priority for the top management, which is trying to achieve the managerial objective with limited resources. Only by doing so can the CISO communicate smoothly with the top management.

(4) Information Protection governance and system of Information Protection organization

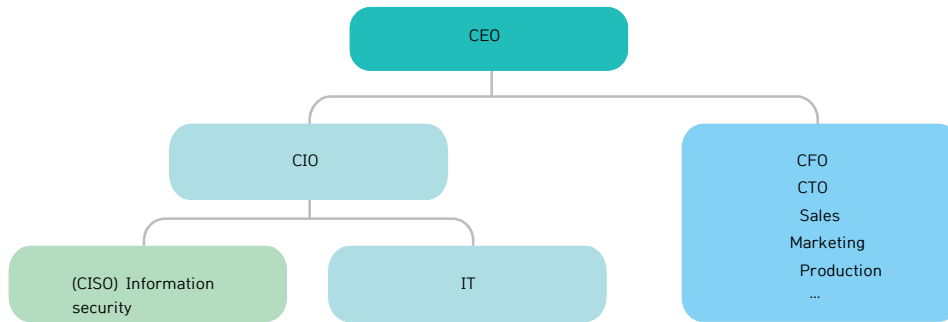
The decisions made by governance are realized through the organizational system. That is why the system of Information Protection organization is important in Information Protection governance. The key factor in Information Protection governance and system of Information Protection organization is the position of the CISO's organization in the organizational system and authorized power. If the system of Information Protection organization composed mainly of the CISO's organization is not organized well for the good performance of the company-wide Information Protection work, it is difficult for the hands-on staff of Information Protection to achieve results even if they work hard, and they only undertake the responsibility for the occurrence of a security problem as they have no authority to make decisions.

Figure 1-10 The system of Information Protection organization - CISO under direct control of CEO



The most desirable system of Information Protection organization in the aspect of Information Protection governance is the one shown in <Figure 1-10>. As a real C-level executive under the direct control of the CEO, the CISO can exercise the authority necessary for company-wide Information Protection and, at the same time, secure the budget and work force, have visibility of the company-wide security risk, and collaborate on company-wide security with ease. If the CISO is neither a C-level executive nor even an executive, being under the direct control of the CEO, such structure of being under the direct control of the CEO can give rise to problems when carrying out company-wide work because the CEO has many managerial agenda items to deal with. Thus, the CISO has to take care of the daily Information Protection work but lacks adequate position and authority.

Figure 1-11 The system of Information Protection organization - CISO under CIO

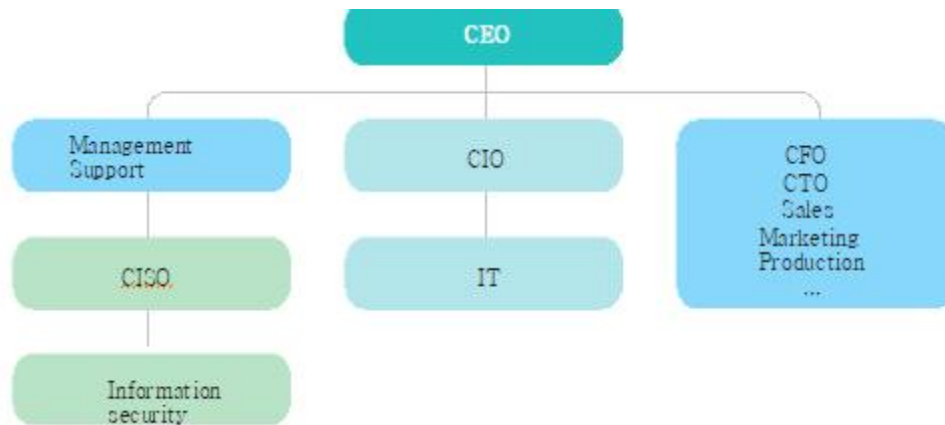


<Figure 1-11> shows a structure of the Information Protection department when the department is first established in a company. As more than half of the Information Protection work is IT security work, the CISO (or the information security department) is positioned under the Chief Information Officer (CIO), or the CIO concurrently serves as the CISO. If the scale of the company is not enough for the establishment of an exclusive team for now, a hands-on worker for Information Protection can be appointed in the IT Operation Team. If the CIO or the IT Operation department has awareness of the security risk to some degree, such organizational structure is helpful in the efficient performance of IT security work.

In some companies, however, the CIO does not have much power. If under the CIO, the CISO may have difficulty in securing the visibility of company-wide security risk or company-wide control. Moreover, the Information Protection department and the IT Operation department sometimes clash while working. While the mission of the IT Operation department is to provide support for the efficient and convenient use of the IT infrastructure by all the departments of the company including the sales and development departments, the Information Protection department is an organization that has to support -- and at the same time control -- all the departments of the company to minimize security risk even if convenience is sacrificed a little. Basically, there is conflict in the nature of their missions.

It is a very normal activity in the company for departments with different roles to find out and solve problems by looking at an issue from different viewpoints. The problem is that such organizational structure may not be proper for the management of security risk. For example, if the CIO fails to report a company-wide security risk of the IT Infrastructure division to the CEO and makes an IT-centered decision or makes a report from the stance of the IT Infrastructure division and leads the CEO to make a wrong judgment, the risk of the IT Infrastructure division can develop into a company-wide risk. Moreover, if the person in charge of Information Protection is working in the IT Operation team, it may be difficult to bring forth a question out of the team.

Figure 1-12 The system of Information Protection organization - CISO under Management Support



As shown in <Figure 1-12>, the CISO's organization can be positioned under the CFO or the Management Support organization such as Management Support division or HR. Some companies put the Information Protection department under the Compliance Officer or the Auditor. At a glance, such organizational structure may look similar to the one in <Figure 1-11>, but the Management Support division is a better environment than the CIO for the CISO's organization to work since it has company-wide visibility and good atmosphere for collaboration and plays the role of certain internal control. Thus, when the CISO's organization reaches a certain size, and its company-wide role becomes important, it is more desirable to have the organizational structure of <Figure 1-12> than the one in <Figure 1-11>.

It is not easy for the CISO to change the Information Protection governance. Note, however, that governance and organizational system are more important than anything else for efficient working in the company. If the organizational structure is not proper for efficient working, the CISO needs to set up and implement plans to change it.

4. The Duty of CISO

(1) The duties of CISO in laws

It is not easy for the CISO to change the Information Protection governance. Note, however, that governance and organizational system are more important than anything else for efficient working in the company. If the organizational structure is not proper for efficient working, the CISO needs to set up and implement plans to change it.

Table 1-1 Paragraph 4 of Article 21-2 of Electronic Financial Transactions Act

Duties of the CISO (Paragraph 4, Article 21-2 of the Electronic Financial Transactions Act)
1. Establishing strategies and plans for securing the stability of electronic financial transactions and protecting the users thereof
2. Protecting the information technology sector
3. Managing human resources and preparing a budget as necessary for the security of the information technology sector
4. Preventing electronic financial transaction incidents and taking measures

We can see that the duties of the CISO in the Electronic Financial Transactions Act are focused on the protection of electronic financial transactions and the security of the IT sector that has realized electronic financial transactions. In a word, security in the Electronic Financial Transactions Act is focused on IT security. In Paragraph 4, Article 45-3 of the Information and Communications Network Act, the duties of the CISO are defined as follows:

Table 1-2 Paragraph 4 of Article 45-3 of Information and Communications Network Act

The duties of the CISO (Paragraph 4 of Article 45-3 of Information and Communications Network Act)
1. Establishment, administration, and operation of an administrative system for information protection
2. Analysis, evaluation, and improvement of the weakness of information protection
3. Prevention of and response to a computer security incident
4. Preparation of preliminary measures for information protection and designing, realization, etc. of security measures
5. Review of preliminary security for information protection
6. Review of encryption of important information and suitability of a security server
7. Other matters, such as taking the necessary measures for the protection of information pursuant to this Act or other relevant statutes or regulations

“Preparation of preliminary measures for information protection and designing, realization, etc. of security measures” (Subparagraph 4) and “Review of preliminary security for information protection” (Subparagraph 5) refer to works that remove any security vulnerability through proper security activities in each stage when implementing new business or service or introducing or developing a new information system including network, server, software, etc. It can be used for the improvement of the existing system, too. There are many similar activities with different names and contents in detail. The figure below shows the “pre-inspection of Information Protection,” which includes a detailed guide.

The ‘Guide for Pre-inspection of Information Protection’ explains pre-inspection of Information Protection as shown in <Figure 1-13>.

Figure 1-13 Pre-inspection of Information Protection



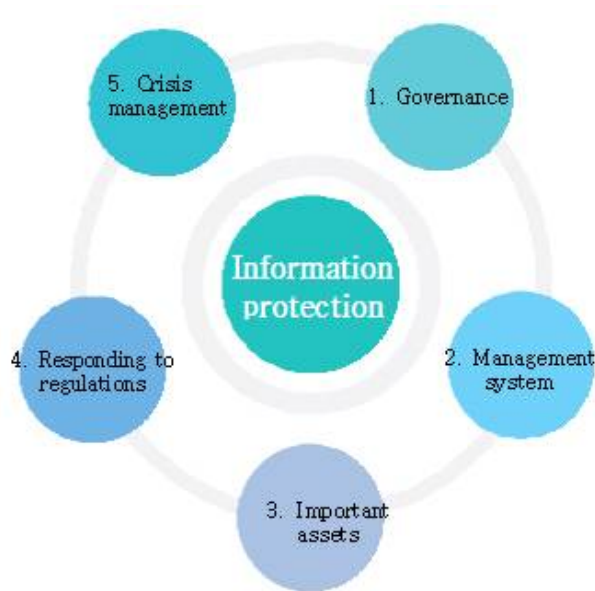
Its purpose is to minimize the security risk of the system by conducting security activities that need to be performed during the stage of establishment of an information system such as planning, analysis/design, realization, test, etc. In contrast, the Information Protection management system (ISMS) is used for the management of security risks during the stage of operation and management following the release of the information system. Similar to that from the viewpoint of software development are “Security by Design,” “Development Security,” “Security Development Lifecycle” as Microsoft’s related methodology, etc.

In the area of software development, it is difficult for CISOs to do more than mock hacking in the test phase because the software development process – the security activities merged in the development process, software security technologies, etc. -- cannot be done easily with the duties or capacity of the CISO's organization. Note, however, that it is possible to solve many of the problems if the security requirements are summarized well during the planning stage or analysis/design stage and managed until the test stage or the operation stage after release of the software.

(2) The duties of the CISO in business entities

The duties of the CISO in the field can be defined as follows.

Figure 1-14 An example of the CISO's Information Protection work



Source: Eun-Seong Kang, "Information security that the CxO Should Know", Hanbit Media, 2015.

As the biggest difference between the duties of the CISO defined here and the ones defined in the relevant laws, Information Protection governance and response to regulations are stated here as the duties of the CISO. Many CISOs are performing works to respond to the laws and regulations related to Information Protection. In particular, in a company retaining customers’ personal information, the CISO, who is carrying out many “technical and administrative protective actions for personal information,” needs to understand fully the relevant laws and regulations or announcements.

The works in the area of governance are already being performed to some degree, but they are not defined as works due to lack of awareness. If there are corporate governance and Information Protection activities, there will be Information Protection governance one way or another, and the top management must be making managerial decisions on major Information Protection policies. The following is an example of Information Protection works in the area of governance:

Table 1-3 Information Protection works in the area of governance (Example)

Work	Details
1. Establish the system under the leadership of the top management	● The top management including the CEO takes responsibility for security risk and establish the system and conducts company-wide communication. ● Appoint and empower an executive level (dedicated) official to take charge of Information Protection
2. Establish a system for communication with the top management and other executives	● Establish a system for key executives to make decisions on the matters related to Information Protection including information security policy, share strategies and policies, and perform company-wide implementation and collaboration. ● Handle Information Protection agenda and communicate in the Executive Meeting, Information Protection Management Committee, etc.
3. Secure Information Protection department/staff/budget	● Establish and empower Information Protection department ● Secure properly sized security staff and security experts ● Secure Information Protection budget
4. Establish and implement Information Protection plans	● Establish Information Protection strategies and plans linked to the managerial objective of the company and collaborate in order to include the Information Protection activities of related departments throughout the company in the business plan of each department ● Minimize the information security risk lurking in the course of achievement of the managerial objective
5. Support Information Protection management	● Assist with the Information Protection agenda of the CEO ● Establish and implement the Information Protection agenda of the CISO ● Support the Information Protection works and activities of other executives

(3) The Information Protection Management Committee: the basis of company-wide collaboration

Among the works in the area of governance, what is necessary for the implementation of company-wide Information Protection work is the establishment of a system for communication with the top management and other executives. Information Protection governance and system of Information Protection organization become the foundation for company-wide collaboration for Information Protection, with the "Information Protection Management Committee" becoming the main body for this.

First, let us take a look at the Information Protection Committee as defined in the Electronic Finance Supervisory Regulations or the Information Security and Personal information protection Management System (ISMS-P) certification.

Table 1-4 Information Protection Committee in the Electronic Finance Supervisory Regulations

Information Protection Committee (Article 8-2 of the Electronic Finance Supervisory Regulations)	
Composition	● Chairperson: CISO ● Members: Head of department related to Information Protection work, Head of department related to operation and development of electronic data processing, Head of department related to compliance work
Role	● Review and resolve the matters about important Information Protection agenda
Works	● Matters about plans in the information technology sector ● Establish strategies and plans to secure stability of electronic financial transactions and protect users ● Matters about analysis and evaluation results of weak points and the plans to implement complementary measures ● Matters about computer security incidents and treatment of those who violate the regulations on computer security ● Other matters decided by the Chairperson of the Information Protection Committee to be subject to information security work

ISMS-P does not contain regulations on the composition of the Information Protection Committee. Note, however, that the "detailed description" of "1.1 Preparation of the basis for management system - 1.1.3 Composition of organization" states something about the Committee. The following is a summary of the contents:

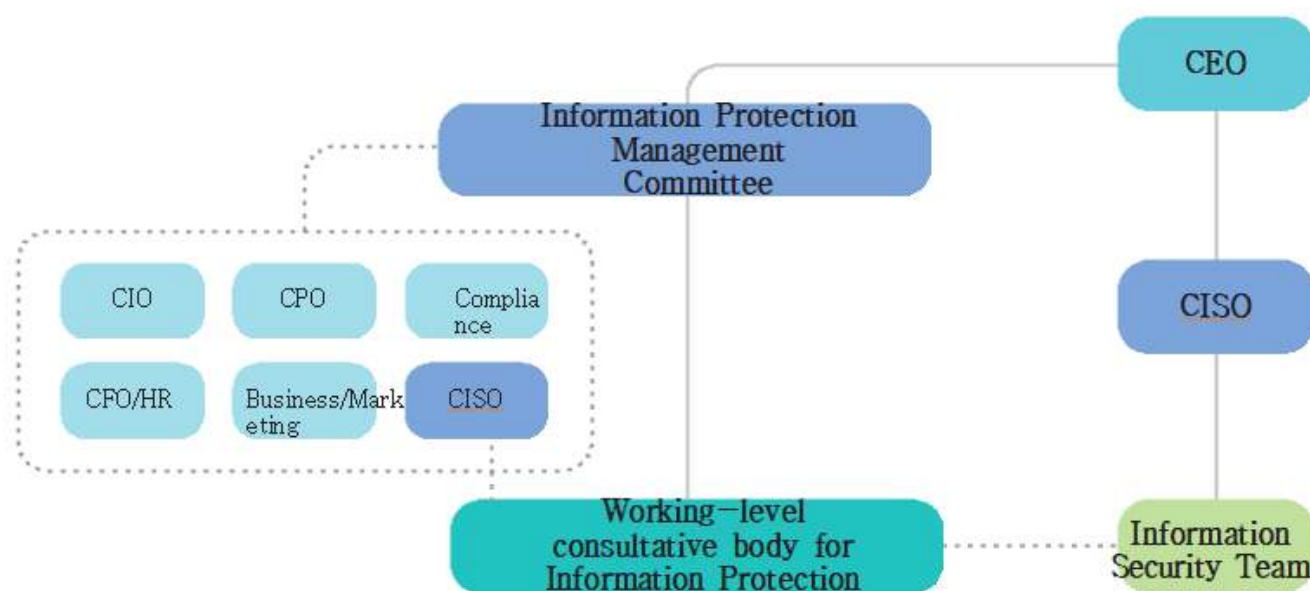
Table 1-5 Information Protection Committee in ISMS-P

Information Protection Committee (ISMS-P)	
Composition	● Committee members: the management, executives, CISO, the officer in charge of personal information protection
Role	● Review, approve and make decisions about the matters related with important information protection throughout the organization
Works	● Establishment and revision of Information Protection and personal information protection policies and guidelines ● Risk assessment results ● Allocation of budgets and resources for Information Protection and personal information protection ● Measures for security incidents and major violations ● Results of internal auditing, etc.

The biggest difference between the Electronic Finance Supervisory Regulations on the Information Protection Committee and ISMS-P lies in the composition of the Committee. In the Electronic Finance Supervisory Regulations, the Information Protection Committee is composed of the heads of departments related to Information Protection instead of executives. If the participants in the meeting are not executives, it is difficult to wield meaningful company-wide influence on the decisions made in the meeting. The participants in the meeting may also try to avoid making any decision that can have a company-wide influence. In contrast, the management and executives are included in ISMS-P, and it is specified as an improper case “if the Information Protection and personal information protection committee has been organized but the Committee is composed of the heads of field working-level departments and, for matters on important information, it is not possible to make any decision on important information of the organization and personal information protection” in order to put emphasis on the participation of executives.

It is necessary to pay attention largely to two things when operating the Information Protection Committee. One is the composition of the Committee, and the other is the agenda. In general, an important decision of the company is made through an approval procedure up to the CEO or in an executive meeting attended by the CEO. In order to make the Committee a company-level decision-making body, the CEO ideally serves as the chairperson of the Committee. That is why the word “management” is included in the name of the Committee - “Information Protection Management Committee.”

Figure 1-15 Composition and operation of Information Protection Management Committee



With respect to the agenda, it is necessary to select agenda items that can make the executives attend the meeting and debate on and participate in decision making such as Information Protection laws and regulations, severe security incident in the company or security incident in another company in the same industry, or major security policy that can have an influence throughout the company. It is better to avoid technical items, if possible. A Committee may not be organized, and the Committee meeting may be replaced with a quarterly executive meeting. What is important is to hold a meeting where the CEO and key executives participate and debate on and decide major Information Protection issues. In order to hold the meeting properly, it is necessary to convene the working-level consultative body for Information Protection to discuss the agenda before the meeting, check the progress of follow-up measures taken for matters decided in the previous meeting, and deliver the decisions of the meeting specifically for the reference of all relevant departments in the company after the meeting.

If the Information Protection Management Committee handles the major agenda items that can affect the works of the company in this way, it becomes possible to discuss and decide the items of collaboration necessary in the process of implementation of company-wide Information Protection work and remove the conflict factors that may occur in the meeting in the process of implementing Information Protection work.

Protection Management Committee will then operate as the main organization for the company-wide collaboration for Information Protection.

Table 1-6 Information Protection Management Committee

Information Protection Management Committee	
Composition	● Chairperson: CEO ● Members: Key executives related to the establishment and execution of company-wide Information Protection policies
Role	● Review and decide major company-wide agenda items for Information Protection from managerial viewpoint
Works	● Make decisions on major company-wide agenda items for Information Protection ● Handle collaboration issues for company-wide Information Protection collaboration ● Make judgment from managerial viewpoint

Table 1-7 Working-level consultative body for Information Protection

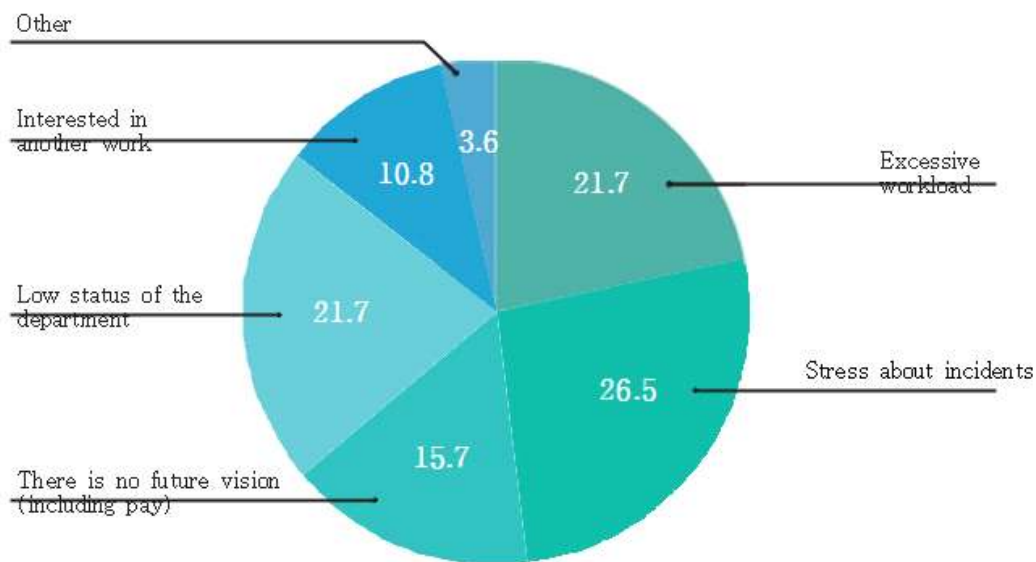
Working-level consultative body for Information Protection	
Composition	● Chairperson: CISO ● Members: Leader of a team related to company-wide Information Protection work or responding to security issues (Team Manager or senior hands-on staff)
Role	● Assist the Information Protection Management Committee and respond to company-wide security issues
Works	● Administrative work such as reviewing the agenda items for the Information Protection Management Committee and taking follow-up measures for decided matters ● Collaboration on Information Protection policies among the persons in charge of working-level affairs ● Quick response to major internal and external security issues

(4) Working-level organization for Information Protection

If possible, the working-level organization for Information Protection is to be organized as a “Team,” which is the basic unit of working-level decision making, because it is difficult to manage company-wide security risks if there is no separate information security team and the person in charge of security belongs to another department. It is even worse if the person in charge of Information Protection is working in the IT operation team controlled by the IT division. Thus, it is advisable to create a team if there are two or more persons; if it is difficult to do so, provide a channel for direct reporting to the CISO so that the CISO can perform company-wide security risk management based on undistorted information. By doing so, the CISO can manage the situation when an urgent security issue occurs.

As expected, the morale of the hands-on staff working for Information Protection in companies is not very high. According to a survey conducted in 2018 by the Council of Computer Emergency Response Teams (CONCERT), a participatory consultative body of security teams or sections of more than 300 Korean companies, the hands-on staff who wanted to change their duties constituted as much as 49%.

Figure 1-16 Reason for desiring to change one's duties



Source: Council of Computer Emergency Response Teams (CONCERT), 2018 Analysis report of the awareness of the persons in charge of corporate Information Protection

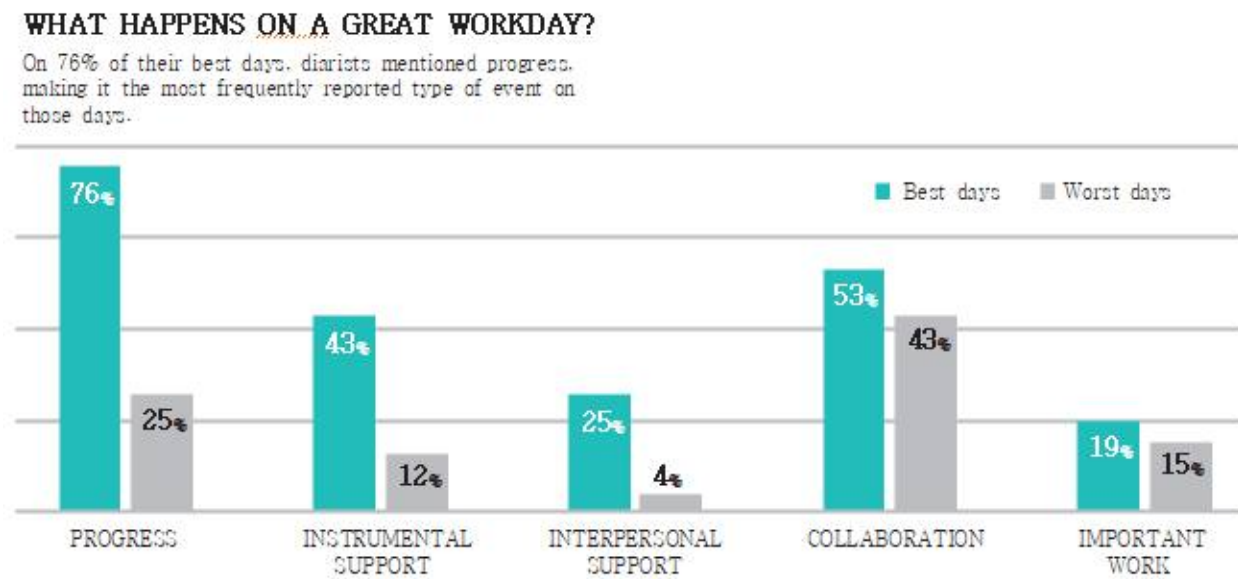
In <Figure 1-16>, the sum of the ratios of “Low status of the department” and “There is no future vision” -- cited as the reason for wishing to change one's duties -- is 37.4%. The two factors are usually caused by the issue of governance. The stress over incidents is also related

to governance as the responsibility for an information security incident structurally falls on the shoulders of the person in charge of Information Protection. Sometimes, the person in charge of Information Protection can be held responsible, but he/she is often not in a position to take responsibility. If the status, authority, and role of the CISO's organization were established, the stress over incidents would not have reached a level that triggered the request for change of duties.

(5) The Best Days vs. The Worst Days

Harvard Business Review (HBR) released a very interesting survey result in 2010. In the previous questionnaire survey on motivation conducted by HBR among 600 managers, the respondents answered that they were motivated by "1. Acknowledgment of their works, 2. Incentive, 3. Support for interpersonal relationship, 4. Support for the implementation of their duties, and 5. A clear goal." The result of the direct survey among hands-on staff was a far cry from the result of the previous survey, however. (There were 269 respondents.)

Figure 1-17 What is the real motivation for workers?



Source: The HBR List: Breakthrough Ideas for 2010, <https://hbr.org/2010/01/the-hbr-list-breakthrough-ideas-for-2010>, Search on Nov. 30, 2019.

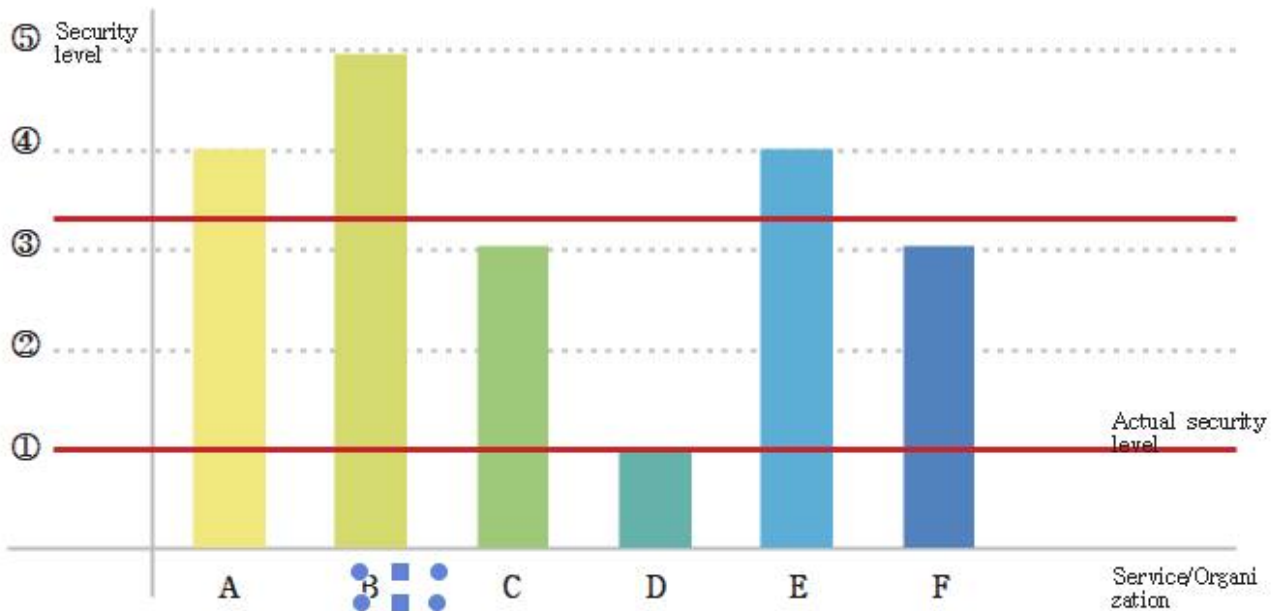
<Figure 1-17> shows the result of analysis of 12,000 e-mails sent from hundreds of knowledge workers every day regarding their motivation and emotion. The biggest reason for the best days was making much progress in their work (76%), and the biggest reason for the worst days was the difficulty in collaboration. By the way, "collaboration" was the second biggest reason for the best days. In other words, the best days were those when the workers performed their work well (with good progress of work), and the worst days were those when they did not perform their work well (with bad collaboration). The survey found out that it was very important for the knowledge workers if they performed their work well or not. The survey result was also different from the previous research of HBR or the "common sense" on motivations for workers. Though it was not possible to infer that the workers had the best days by motivation, it proved that there was correlation between the two factors.

A characteristic of collaboration is that we cannot make progress in work if we simply work hard alone, but we can get it done by working hard together with the support of the collaboration partner. Usually, collaboration cannot be done fully with only the personal capacity of hands-on staff and is often instructed by the CEO, executives, and department heads who are in key positions in the governance and organizational system and the collaboration system. In the collaboration for Information Protection, the role of the CISO is more important than anything else. Just as important as preparing the aforementioned organizational system is for the CISO to define collaboration management as his/her duty and perform it. Such will then certainly motivate the members of the department to work well.

5. Conclusion

Various methods are used in the evaluation of the security level of a company, and one of them is scoring the security levels of many areas and calculating the average.

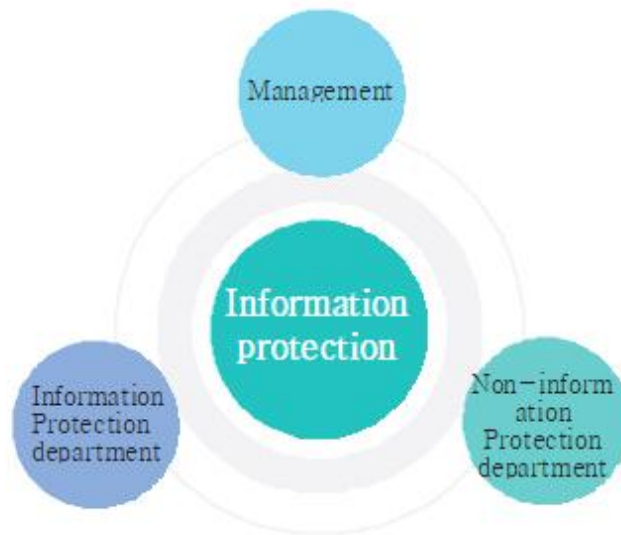
Figure 1-18 Security level of a company



For example, suppose Information Protection policy (A) is given 4 points, outsider security (B) is given 5 points, employee security (C) is given 3 points, server security (D) is given 1 point, network security (E) is given 4 points, and website security (F) is given 3 points; the average security of the company becomes 3.3 points. Such method is helpful in understanding the general security level of a company but not very helpful in finding out the vulnerable areas and preventing security incidents because incidents usually occur in the D area, which is well below the average. Thus, it is appropriate to give one point to the actual security level of the company from the viewpoint of the CISO. The most urgent task of the CISO is to find out an area with a very low security level like the D area and improve the level to the average level at least.

There is an easy way to find out an area with low security level. The hands-on staff are already aware of much of the fact. Talk frankly with the people who are conversant with the Information Protection policy of the company and the solutions such as the hands-on security staff, IT system operators, and developers to grasp the actual situation. Doing so also enables identifying the company's important assets that need to be protected and the items targeted by criminals.

Figure 1-19 Three principle agents of Information Protection in a company



As we have examined so far, the Information Protection department and the Non-Information Protection departments should collaborate on the basis of the Information Protection governance led by the top management for the systematic execution of Information Protection activities. The CISO and the Information Protection department, too, must communicate and collaborate actively for this purpose.



the CISO

Guidebook

Basic

II

CISO's Awareness



1. The Laws that CISO should know
2. The Security that CISO should know

1. The Laws that CISO should know

Which law in relation to Information Protection can be applied to a company publicizing its products through the homepage without running a membership program? If an infringement incident occurs in the homepage, will the company be free from legal liability if it solves the problem by itself without making a report? If a start-up company runs a simple blog for PR without a company homepage or a membership program, is there no law on Information Protection applicable to the company? It is not easy for the CISO to answer these questions clearly.

The representative laws related to Information Protection and personal information protection applicable to business entities are the "Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (hereinafter referred to as "Information and Communications Network Act")" and "Personal Information Protection Act." Some CISOs may think that they need not observe the Information and Communications Network Act if they do not collect personal information through their homepage. Note, however, that the purpose of establishment of the Information and Communications Network Act is to "promote the safe use of the information and communications network" and "protect the personal information of the people who use the information and communications service (the users)." Even if the homepage is being operated for a simple purpose, it is necessary to observe the Information and Communications Network Act as it can affect the safe use of the information and communications network.

In 2018, the National Assembly passed the amendment to the "Information and Communications Network Act" to prohibit the CISO from holding more than one office and decide the qualification requirement of the CISO by a Presidential Decree. According to the law, more than 34,000 companies including mid-sized and large companies providing information and communications services, all telecommunication carriers excluding value-added common carriers with capital of less than KRW 100 million, and information and communication service providers that must be certified by the Information Protection management system (ISMS) are required to appoint a CISO and report it to the Minister of Science and ICT.

Under legal requirement, business entities must appoint a CISO. According to the qualification requirement, the CISO is required to have a degree and work experience in Information Protection or information technology. At a company where it is prohibited for the CISO to hold an additional position, the CISO must have working experience of more than 4 years in Information Protection area or more than 5 years of total career in the areas of Information Protection and information technology with at least 2 years of working experience in Information Protection area.

Even if the CISO has a career in Information Protection area or related areas, the following capacity is required for safe protection of the organization from advanced and intelligent threats to Information Protection.

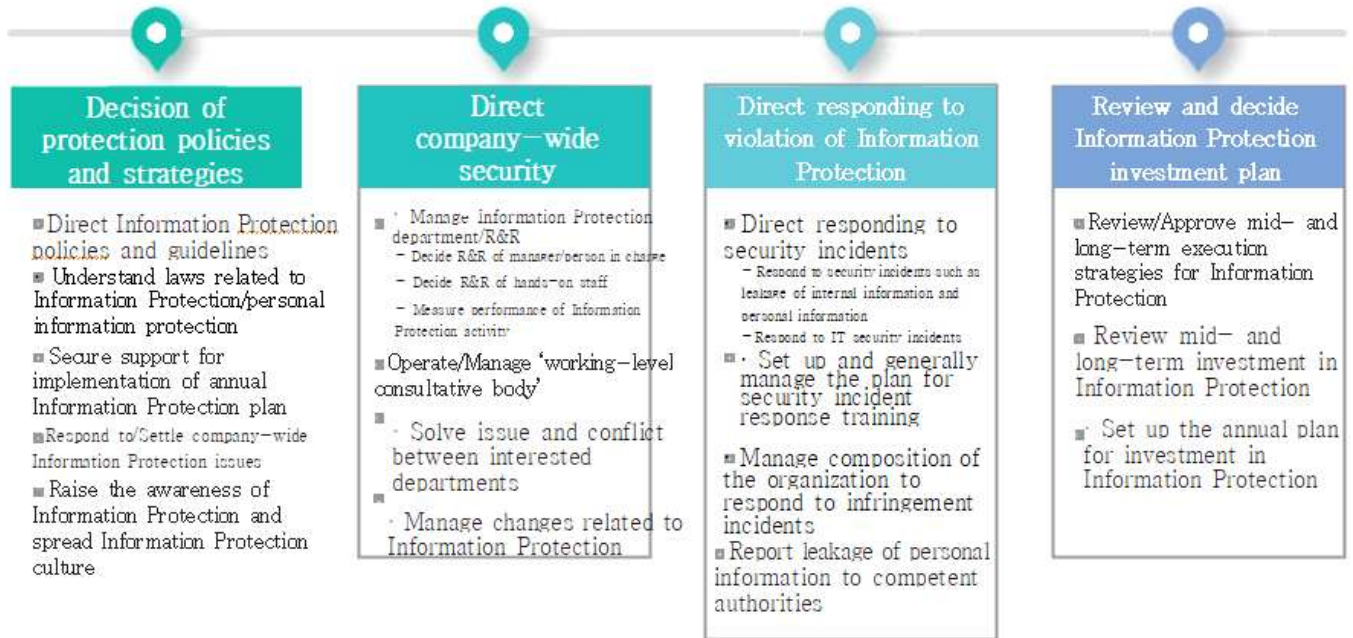
- Understanding of the key businesses of the organization
- Understanding of the laws on information security related to the businesses of the organization
- Grasping the regulation trend of the government and other public agencies related to Information Protection
- Identifying the stakeholders related to Information Protection and adjusting a conflict of interest
- Managerial and technical security knowledge related to Information Protection

The CISO must have a good understanding of the business of the organization and promote internal communication in order to explain the contents related to the information security of the organization to the management sufficiently and receive support. As the legal and systematic requirements related to Information Protection are being strengthened continuously, it is necessary to identify them, analyze their influence on the organization, and communicate with the management about the matters necessary to be reflected to the organization's Information Protection regulations.

In order to realize and implement the Information Protection management system of the organization, the Information Protection department, the IT department, and the field department need to cooperate closely, and a conflict of interest may occur frequently due to the work of the Information Protection department to control, inspect, audit and monitor the IT department and the field department. In relation to this, the CISO must be able to solve the conflict of interest to reach a compromise between the business of the organization and Information Protection and has a good understanding of managerial and technical security for effective and continuous implementation of the Information Protection management system and prevention of incidents.

Then, what are the responsibility and role of the CISO? [Figure 2-1] below is an example of it.

Figure 2-1 Responsibility and role of the CISO



(1) Laws applied to business entities

The following are the kinds of laws applicable to different businesses of the organization.

Table 2-1 Laws on Information Protection

Area	Applicable law
Information Protection and personal information protection	● Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. ● Personal Information Protection Act ● Act on the Protection of Information and Communications Infrastructure ● Act on the Protection, use, etc. of Location Information ● Unfair Competition Prevention and Trade Secret Protection Act ● Act on Prevention of Divulgence and Protection of Industrial Technology
Finance	● Credit Information Use and Protection Act ● Electronic Financial Transactions Act
Employment of workers	● Labor Standards Act ● Fair Hiring Procedure Act
Others	● Framework Act on Electronic Documents and Transactions ● Digital Signature Act ● Protection of Communications Secrets Act

In this text, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (hereinafter referred to as 'Information and Communications Network Act') and the Personal Information Protection Act' will be mainly examined as they must be observed essentially for protection of corporate information and personal information.

Item	Information and Communications Network Act	Personal Information Protection Act
Division	Special law	General law
Scope of application	To be applied unless there is a different special provision on promotion of information and communications network utilization and information protection, etc.	To be applied unless there is a special provision on protection of personal information in other laws
Object of application	Information and communications service provider (A business operator offering services for profit-making)	Personal information processor (An organization/corporation/group/person that processes personal information for business)
Object of protection	User (A person who uses information and communications service)	Principal of information (A person who can be identified by processing of information)
Consent to collection	Consent	Consent
Consent to consignment	Consent	Notice
Consent to transfer	Consent	Consent
Provision of personal information	Consent	Consent
Restriction to transmission of advertising information for profit-making	Can be transmitted with a consent	-
Installation and operation of visual data processing devices	-	Take necessary measures such as installation of a signboard
Personal information impact assessment	-	To be applied only in public agencies

Table 2-2 Comparison of Information and Communications Network Act and Personal Information Protection Act

The following are the examples of the laws applied to different business types.

Type 1	If the product PR and recruitment sites are maintained through the homepage and employees are hired offline → Information and Communications Network Act(homepage), Personal Information Protection Act(employment)
Type 2	If personal information is collected offline from POS, etc. and marketing is conducted through text message and e-mail using the collected information → Information and Communications Network Act(marketing through text message/e-mail), Personal Information Protection Act(Collection of personal information from POS)
Type 3	If the personal information and bonus points collected from the written application and contract are inquired in the homepage and used for purchase of products → Information and Communications Network Act(Inquiry about contract information and purchase of products in the homepage), Personal Information Protection Act(Collection of personal information from the written application and contract)
Type 4	If an event is held through the SNS → Information and Communications Network Act

(2) Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

The Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (The Information and Communications Network Act) is applied to information and communications service providers, and was enacted to 'protect personal information of people using information and communications services' and develop an environment in which 'people can utilize information and communications networks in a safer way'.

Article 1 (Purpose) The purpose of this Act is to contribute to improving citizens' lives and enhancing public welfare by facilitating utilization of information and communications networks, protecting personal information of people using information and communications services, and developing an environment in which people can utilize information and communications networks in a healthier and safer way.

Therefore, an information and communications service provider must take managerial and technical protective measures in order to protect the personal information of the people who use the information and communication service safely; report any leakage of the personal information of users; and make a report to the competent authorities if the homepage in operation has been falsified or a malignant code is found.

The following are the definitions of the terms frequently mentioned in Information and Communications Network Act.

Article 2 (Definitions) ① The definitions of the terms used in this Act shall be as follows:

1. The term "information and communications network" means an information and communications system for collecting, processing, storing, searching, transmitting, or receiving information by using telecommunications equipment defined in subparagraph 2 of Article 2 of the Telecommunications Business Act or computers and applied computer technology.
2. The term "information and communications services" means telecommunications services defined in subparagraph 6 of Article 2 of the Telecommunications Business Act and services providing information or intermediating the provision of information by using such telecommunications services.
3. The term "provider of information and communications services" means a telecommunications business entity defined in subparagraph 8 of Article 2 of the Telecommunications Business Act and any other person who provides information or intermediates to provide information commercially by utilizing services provided by a telecommunications business entity.
4. The term "user" means a person who uses information and communications services rendered by providers of information and communications services.
5. The term "electronic document" means data prepared and transmitted, received, or stored electronically in a standardized document by a device capable of processing information, such as a computer.
6. The term "personal information" means information pertaining to an individual alive, which contains information identifying a specific person with a name, a national identification number, or similar in the form of a code, letters, voice, sound, motion picture, or any other form (including information that makes it impracticable to identify a specific person by itself, but that enables to identify such person easily if combined with another information).
7. The term "computer security incident" means an event resulting from an attack on an information and communications network or an information system related to such network by means of hacking, computer virus, logic bomb, electronic mail bomb, denial of service, high-power electromagnetic wave, etc.

Included in the definition of information and communication service provider in Information and Communications Network Act is 'any other person who provides information or intermediates to provide information commercially by utilizing services provided by a telecommunications business entity'. Thus, if a person operates the homepage for the purpose of PR of products is regarded as providing information for profit-making and shall be applied by Information and Communications Network Act.

The following table shows the composition of Information and Communications Network Act, and the chapters that claim our attention are 'Chapter 4. Protection of personal information', 'Chapter 6. Securing of stability of information and communications network', etc.

Table 2-3 Major contents of Information and Communications Network Act

Chapter	Major concepts
Chapter 1. General Rules	● Purpose of the act, definition of terms, and definition of relations with other laws ● Relations with other laws
Chapter 2. Promotion of utilization of information and communications network	● Standardization of information and communications network, designation of certification agency, etc. ● Business on promotion of utilization of information and communications network, etc. and spreading use of the Internet
Chapter 3. Deleted	● Deleted on June 22, 2015
Chapter 4. Protection of personal information	● Collection, use and provision of personal information ● Management, destruction, etc. of personal information ● Users' rights
Chapter 5. Protection of users, etc. in information and communications network	● Indication of the media materials harmful to teenagers and prohibition of their advertisement ● Protection of rights, request for deletion of information, etc. in information and communications network, ● Identification of users in bulletin board and demanding provision of user information ● Prohibition of distribution of illegal information
Chapter 6. Securing safety of information and communications network, etc.	● Secure safety of information and communications network, etc. ● Advance inspection of Information Protection, appointment of CISO, etc. ● Protect integrated information and communication facilities ● Certification of Information Protection management system and personal information protection management system ● Protect user information and assign Information Protection management level ● Prohibit infringement of information and communications network, respond to security incidents, report infringement incidents, analyze cause of infringement incidents, etc. ● Restrict transmission or posting of advertisement information for profit-making ● Restrict outflow to abroad of important information, etc..
Chapter 7. Communication charging service	● Register communication charging service provider, etc. ● Securing safety in communication charging service, users' rights in communication charging service, etc. ● Mediate and settle disputes; compensate for damages, etc.
Chapter 8. International cooperation	● International cooperation ● Protect personal information from cross border transfer

When a company is going to collect and use the personal information of users, the company needs to notify the following matters to the users and receive their consent. It is the same when there is a change.

- ❶ The purpose of collection and use of the personal information
- ❷ The items of personal information being collected
- ❸ The period of retention and use of the personal information

If it is difficult to receive usual consent to the collection and use of the personal information necessary for fulfillment of the contract for provision of information and communication service due to economic or technical reasons; if it is needed for calculation of charges for provision of information and communication service; or if there is a special provision in another law, it is possible to collect and use personal information without consent of the user. If the personal information of a child under 14 of age, it is required to receive the consent of the legal representative of the child and use an easy form and linguistic expression so that the child could

easily understand the notice on the processing of the personal information.

When collecting the personal information of users, the relevant company shall collect only the minimum personal information necessary for provision of the information and communication service of the company, and the responsibility for proving collection of the minimum personal information lies with the relevant company. The relevant company may not refuse provision of the service on the grounds that the user does not provide some personal information in addition to the minimum necessary personal information.

If a company consigns collection, creation, connection, linkage, recording, storage, retention, processing, editing, search, printing, correction, recovery, use, provision, opening, destruction, etc. (hereinafter referred to as "processing") of the personal information of a user to a third party (hereinafter referred to as "consignment of processing of personal information"), it is required to notify the user of ❶ the person who is consigned for processing of the personal information and ❷ the contents of the personal information consigned for processing and receive the consent of the user. It is the same when there is a change. In addition, the relevant company shall state the purpose of processing of the personal information of the user by the consigned company in documents including the contract and supervise and educate the consigned company not to violate the Information and Communications Network Act and the contract. Most companies check the observance of the obligation of personal information protection by the consigned company once a year and evaluate the performance by site inspection, questionnaire survey, etc. considering the type and size of the consigned company, the characteristic of the processed personal information, etc. If the consigned company wishes to re-consign the personal information to a third party, it is required to receive the consent of the consigning company without fail.

For processing of the personal information of users, the personal information processing policy shall be announced publicly in the homepage, etc. including the following matters. In addition, when the personal information processing policy is changed, the reason for and contents of the change shall be announced without delay and measures shall be taken to let the users be aware of the change anytime.

- The purpose of collection and use of personal information, the items of collected personal information, and the collection method
- If the personal information is being offered to a third party, the name (corporation name) of the recipient, the purpose of use of the recipient, and the items of offered personal information
- The period of retention and use of personal information and the procedure and method of destruction of personal information (including the ground for preservation of personal information and the items of preserved personal information if personal information is preserved)
- The contents of work and consigned company if processing of personal information is consigned
- The rights of the user and the legal representative and the method of exercise of the rights
- Matters about installation and operation of the device which collects personal information automatically such as the Internet access information file and its refusal
- The name, telephone number or other contact information of the person in charge of personal information protection or the department handling personal information protection work and related grievances

The personal information processing policy is prepared for the purpose of informing the methods and procedures used for safe protection and destruction of the personal information of the user being collected and used by the relevant organization and the name and contact information of the person in charge of management. The personal information processing policy must be explained in detailed for the items stated in laws referring to the major contents of the guidelines of the company for protection of personal information. As the items of personal information being collected and used, the consigned company, a third party which is offered the personal information, etc. may vary according to the character of the service, it is necessary to check them regularly and reflect changes to the processing policy.

The following technical and managerial protective measures shall be prepared and implemented in order to prevent loss, theft, leakage, forgery, falsification or damage to the personal information of user when the personal information is processed.

- Prepare and implement internal management plan to process personal information in a safe way.
- Install and operate access control device such as the firewall to block illegal access to personal information.
- Measures to prevent forgery/falsification of the method of access
- Security measures using encryption technology for safe storage and transmission of personal information
- Measures to prevent intrusion by computer virus including installation and operation of vaccine software
- Other protective measures necessary for securing safety of personal information

A company which is subject to Information and Communications Network Act shall prepare the internal personal information management plan according to the act. The internal personal information management plan shall include the following matters, and it is recommended to revise the plan once a year after reviewing it as the plan contains the plan for training of personal information handlers.

- Matters about composition and operation of personal information protection organization including appointment of the person responsible for processing the personal information of users (the persons handling personal information)
- Install and operate access control device such as the firewall to block illegal access to personal information.
- Measures to prevent forgery/falsification of the method of access
- Security measures using encryption technology for safe storage and transmission of personal information
- Measures to prevent intrusion by computer virus including installation and operation of vaccine software

The following measures must be taken to block illegal access to personal information: ① preparation and implementation of the standards for granting, changing, terminating, etc. the access authority to the personal information processing system; ② installation and operation of the firewall and intrusion detection system for the personal information processing system; ③ blocking outside Internet network from the computer, etc. of personal information handlers

connecting with the personal information processing system; ④ setting and operating the standards for the creation method, cycle of change, etc. of the password; and ⑤ the measures necessary for control of access to personal information. However, ③ blocking outside Internet network from the computer, etc. of personal information handlers is applied only to the companies with more than average one million users a day for the past 3 months as of the end of the last year or over KRW 10 billion of sales in the sector of information and communication service during the previous year.

For prevention of forgery/falsification of personal information processing system access logs, ① the date and time of access to the personal information processing system and the details of processing must be stored with review of the logs and ② the access logs of the personal information processing system must be stored in separate backup equipment. Also, it is necessary to check the following extraordinary activities when reviewing the personal information processing system access logs and processing logs: excessive attempt to access, attempt to access after business hours; excessive inquiry/download/output, excessive attempt to remove masking; turning off encryption excessively; inquiry after business hours, etc. For safe storage/transmission of personal information, security measures must be taken by ① one-way encryption of the password, ② encryption of resident registration number, bank account information, bio information, etc. and ③ installation of the security server when sending and receiving users' personal information and authentication information through the information and communications network. It is necessary to make sure that a safe encryption algorithm is used and check the length of the encryption key regularly. For the security server, it is necessary to check the expiration date of the authentication certificate and the appropriateness of the encryption algorithm.

If the purpose of collection/use of a user's personal information has been achieved; if the period of retention and use of the personal information has expired; or the relevant business is closed, the relevant personal information must be destroyed in an irreversible/nonrenewable way without delay. However, if the personal information is required to be preserved by another law, it may be kept for a certain period stipulated by the relevant law.

Table 2-4 Period of retention of personal information according to other laws

Item	Retention period
Records on contracts or withdrawal of application	5 years
Records on price payment and supply of goods, etc.	5 years
Records on settlement of consumer complaints or disputes	5 years
Records on labeling/advertisement	6 months

In order to protect the personal information of the users who haven't used the information and communication service for over a year, ① the personal information of such users must be destroyed promptly or ② it should be stored separately from the personal information of other users. Even if the information is stored separately, it is necessary to prepare internal standards to establish the procedure to destroy it after storing it for a certain period of time. The separately stored personal information must be managed safely to prevent illegal use or provision, and the fact of impending destruction of the personal information, the expiration date, the items of personal information to be destroyed, etc. must be notified to the users via e-mail, etc. at least 30 days before the expiration date.

As the users may withdraw their consent to the collection, use, provision, etc. of their personal information anytime, it is necessary to establish the procedure to guarantee the right and the relevant personal information must be destroyed in an irreversible/nonrenewable way without delay. In addition, the users may demand perusal or provision of the status of processing of their personal information and request correction if there is any errors.

① The personal information of users being retained

② The status of use of personal information of users or provision of the personal information for a third party

③ The status of consent to collection/use/provision, etc. of personal information

The details of use of the personal information of users must be notified to the users once a year including ① the purpose of collection and use of personal information and the items of collected personal information, ② the recipient of the personal information, the purpose of provision and the items of provided personal information, and ③ the person consigned for processing of personal information and the contents of consigned works via e-mail, written documents, fax, telephone, etc.

(3) Personal Information Protection Act

Personal Information Protection Act is applied to all personal information controllers, and was enacted to protect the freedom and rights of individuals by prescribing the processing and protection of personal information.

Article 1 (Purpose) The purpose of this Act is to protect the freedom and rights of individuals, and further, to realize the dignity and value of the individuals, by prescribing the processing and protection of personal information.

The Information and Communications Network Act is a special law applied to information and communication service providers and Personal Information Protection Act is a general law applied to personal information controllers including corporations, public agencies and individuals that process personal information for their working. Thus, an information and communication service provider must observe the matters prescribed in the Information and Communications Network Act first and then observe the matters not prescribed in the Information and Communications Network Act such as 'handling visual data processing devices' according to Personal Information Protection Act.

The following are the definitions of the terms frequently mentioned in Personal Information Protection Act.

Article 2 (Definitions) ① The terms used in this Act shall be defined as follows:

1. The term "personal information" means any of the following information relating to a living individual:
 - (a) Information that identifies a particular individual by his or her full name, resident registration number, image, etc.;
 - (b) Information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. In such cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured;
 - (c) Information under items (a) or (b) above that is pseudonymized in accordance with subparagraph 1-2 below and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state (hereinafter referred to as "pseudonymized information");
- 1-2. The term "pseudonymization" means a procedure to process personal information so that the information cannot identify a particular individual without additional information, by deleting in part, or replacing in whole or in part, such information;
2. The term "processing" means the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, searching, output, correction, recovery, use, provision, disclosure, and destruction of personal information and other similar activities;
3. The term "data subject" means an individual who is identifiable through the information processed and is the subject of that information;
4. The term "personal information file" means a set or sets of personal information arranged or organized in a systematic manner based on a certain rule for easy search of the personal information;
5. The term "personal information controller" means a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities;
6. The term "public institution" means any of the following institutions:
 - (a) The administrative bodies of the National Assembly, the Courts, the Constitutional Court, and the National Election Commission; the central administrative agencies (including agencies under the Presidential Office and the Prime Minister's Office) and their affiliated entities; and local governments;
 - (b) Other national agencies and public entities prescribed by Presidential Decree;
7. The term "visual data processing devices" means the devices prescribed by Presidential Decree, which are continuously installed at a certain place to take pictures of persons or images of things, or transmit such pictures or images via wired or wireless networks.

There are several terms in Personal Information Protection Act used differently from Information and Communications Network Act such as ① data subject (‘user’ in Information and Communications Network Act) and ② personal information controller (‘information and communication service provider’ in Information and Communications Network). Thus, it is necessary to use appropriate terms according to the applied laws. Also, the term personal information controller must be differentiated from the term personal information handler. A personal information controller means the corporation using personal information files for its work, which is a company, while a personal information handler means an executive or employee who belongs to the personal information controller and handles personal information.

The following table shows the composition of Personal Information Protection Act.

Table 2-5 Major contents of Personal Information Protection Act

Chapter	Major contents
Chapter 1. General Rules	● Purpose of the act, definition of terms and definition of relations with other laws ● Relations with other laws
Chapter 2. Establishment of personal information protection policy	● Personal Information Protection Committee and the function of Personal Information Protection Committee ● Demand for submission of data, Guidelines for personal information protection, international cooperation
Chapter 3. Processing of personal information	● Collection and use of personal information; restriction to collection of personal information ● Provision of personal information; restriction to use/provision of personal information other than the original purpose ● Destruction of personal information ● Restriction to processing sensitive information; restriction to processing unique identification information; restriction to processing resident registration number ● Restriction to installation and operation of visual data processing devices ● Restriction to processing personal information by business consignment
Chapter 4. Safe management of personal information	● Supervision of personal information handlers ● Establishing and publicizing the responsibility for safety measures and privacy policy ● Appointment of the person responsible for personal information protection ● Certification for personal information protection; personal information impact assessment
Chapter 5. Guaranteeing the rights of data subjects	● Notification of leakage of personal information, etc.; imposition of surcharge, etc. ● Perusal of personal information; correction and deletion of personal information ● Suspending processing of personal information, etc.
Chapter 6. Personal Information Dispute Mediation Committee	● Method and procedure of exercise of rights; liability for damages ● Establishment and composition of the Committee; guarantee of status of committee members, application for mediation, etc. ● Processing period, request for data, etc.; recommendation for agreement before arbitration; mediation of disputes
Chapter 7. Group litigation on personal information	● Object, etc. of group litigation; exclusive jurisdiction ● Appointment of litigation representative, application for litigation permit, litigation permit requirement, etc. ● Dispute mediation and settlement, etc.; compensation for damages, etc.

If a personal information controller is going to collect and use the personal information of a data subject, it is necessary to notify it to the data subject and obtain consent of the data subject. It is the same when there is a change.

- ❶ The purpose of collection and use of personal information
- ❷ The items of personal information being collected
- ❸ The period of retention and use of the personal information
- ❹ The fact that the data subject has the right to refuse and the contents of disadvantages if there are disadvantages resulting from refusal to consent

When collecting personal information, the personal information controller shall collect only the minimum personal information necessary for the original purpose, and the responsibility for proving collection of the minimum personal information lies with the personal information controller. The personal information controller may not refuse provision of the service for the data subject on the grounds that the data subject does not consent to collection of personal information.

The personal information controller may provide the personal information of the data subject for a third party with the consent of the data subject. When obtaining the consent of the data subject, the personal information controller must notify the data subject of the following matters. A new consent must be obtained if there is any change in the matters to which the data subject consented. It is the same when the personal information is provided for a third party located abroad.

- ❶ The person who is offered the personal information
- ❷ The purpose of use of the personal information by the person who is offered the personal information
- ❸ The items of personal information being offered
- ❹ The period of retention and use of the personal information by the person who is offered the personal information
- ❺ The fact that the data subject has the right to refuse and the contents of disadvantages if there are disadvantages resulting from refusal to consent

The personal information controller may not use or offer to a third party the personal information beyond the scope of purpose of its collection and use. The personal information controller must destroy the relevant personal information in an irreversible/nonrenewable way without delay if the retention period expires or the relevant personal information becomes unnecessary by achievement of the purpose of processing the personal information. However, if the personal information is required to be preserved by another law, it may be kept separately by the personal information of other data subjects for a certain period stipulated by the relevant law.

In order to obtain the consent of the data subject (including the legal representative) to the processing of personal information, it is necessary to obtain the consent separately by dividing the

matters that need consent so that the data subject can recognize them clearly. When the consent is going to be obtained in a written form (including an electronic document), the purpose of collection and use of personal information, the items of personal information being collected and used, etc. must be stated clearly for easy understanding. When obtaining the consent to the processing of personal information for the purpose of PR or recommendation of sale to the data subject, it is necessary to make sure that the data subject is clearly aware of it before obtaining the consent. In order to obtain consent for the processing of the personal information of a child under 14 of age, it is required to obtain the consent of the legal representative of the child. It is allowed to collect the minimum information needed for obtaining the consent of the legal representative directly from the relevant child without the agreement of the legal representative.

The personal information controller must obtain a separate agreement of the data subject for collection of the data subject's thoughts, belief, membership of labor union or political party, political opinions, health, sexual life, and other kinds of personal information (sensitive information) that can infringe upon the privacy of the data subject significantly or shall not collect/use such information unless it is permitted by relevant laws. It is also necessary to obtain a separate agreement of the data subject for collection of the data subject's unique identification information (driver's license number, passport number, and foreign registration number) or shall not collect/use such information unless it is permitted by relevant laws. If unique identification information is collected/used, it is necessary to take safety measures such as approval of the responsible person, access authorization, etc. at the time of encryption, masking, unmasking, etc. in order to prevent loss, theft, leakage, forgery, falsification, or damage of the relevant unique identification information. It is not allowed to process resident registration number unless it is permitted by law.

It is not allowed to install and operate visual data processing devices (CCTV) at a place which can watch the inside of a space of privacy such as a restroom or a locker room that are used by many and unspecified persons. A person who install and operate visual data processing devices (visual data processing devices operator) shall install a signboard telling the purpose and location of installation, the coverage and time, explanation and contact information of the person in charge, etc. for easy recognition and understanding of the data subject. Visual data processing devices may not be operated for purposes other than the original purpose or shoot other spots or use the sound recording function.

If the personal information controller consigns the processing of the personal information to a third party, the following items must be included in documents including the contract, etc.

- ❶ Prohibition of the processing of personal information for purposes other than the purpose of execution of the consigned work.
- ❷ Technical and managerial protective measures for personal information
- ❸ Purpose and scope of consigned work

- ④ Restriction of re-consignment
- ⑤ Measures to secure safety such as restriction of access to personal information
- ⑥ Matters about supervision such as inspection of the status of management of the personal information being retained for consigned work
- ⑦ Responsibility including compensation for damage of the consignee in case the obligation of the consignee is not observed

The personal information controller shall publicize the contents of consigned work and the consigned company in the homepage, etc. for easy recognition of the data subject. If the information cannot be posted in the homepage, it shall be posted at a place easy to be seen such as the workplace; publish it in the newspaper; use the newsletter, PR materials or bills issued and distributed at least twice a year; or include it in a contract, etc. prepared by the consignor and the data subject and issued to the data subject. The consignor must educate the consignee to prevent loss, theft, leakage, forgery, falsification or damage of the personal information and manage and supervise safe processing of the personal information by the consignee through regular inspection of the status of processing.

The personal information controller shall manage and supervise the personal information handler properly and conduct education necessary for guaranteeing appropriate handling on a regular basis.

When processing the data subject's personal information, it is necessary to publicize the policy of processing of personal information including the following matters in the homepage, etc. If there is a change in the policy of personal information processing policy, the reason and contents of the change shall be announced without delay and measures shall be taken in order to let the users recognize the changes anytime.

Purpose of processing personal information
 Items of the personal information being processed
 The period of processing and retention of personal information
 Matters about provision of personal information for a third party (if applicable)
 Matters about consignment of personal information processing (if applicable)
 The rights and obligations of the data subject and the legal representative and how to exercise the rights
 The name of the person responsible for protection of personal information or the department in charge of protection of personal information and related grievances and the telephone number or other contact information
 Matters about installation and operation of the devices collecting personal information automatically such as the Internet access information file and its refusal (if applicable)
 Matters about destruction of personal information
 Matters about the measures taken for securing safety of personal information

The personal information controller shall appoint a person responsible for personal information protection who will take charge of the processing of personal information. The person responsible for personal information protection are required to perform the following works, and will not be

given disadvantages for performance of the duties without a justifiable reason.

- ❶ Establishment and execution of personal information protection plan
- ❷ Regular inspection of the status and practice of personal information processing and their improvement
- ❸ Handling complaints and relieve damages related to processing personal information
- ❹ Establishment of internal system for prevention of leakage and misuse/abuse of personal information
- ❺ Establishment and execution of personal information protection and education plan
- ❻ Management and supervision of protection of personal information files
- ❼ Establishment/change of personal information processing policy
- ❽ Management of the data related to personal information protection
- ❾ Disposal of the personal information whose purpose of processing has been achieved or retention period has expired

If the person responsible for personal information protection comes to know a violation of law in relation to the protection of personal information, he/she must take improvement measures and, if necessary, report the improvement measures to the management.

If it is found out that personal information has been leaked out, the personal information controller shall notify the relevant data subject of the following things without delay.

- ❶ The item(s) of leaked personal information
- ❷ The time and cause of leakage
- ❸ The information on what the data subject can do to minimize the damages that may be inflicted due to the leakage
- ❹ Countermeasures of the personal information controller and the process of relief
- ❺ The telephone number, etc. of the department in charge or receipt of reports if the data subject has suffered damages

The personal information controller shall establish the procedures to respond to personal information leakage incidents in order to prepare the measures to minimize damages in case personal information is leaked out. A written script has to be prepared for the counselors at the customer center to cope well if a personal information leakage incident occurs; there must be a single department to function as an external communication channel; and analyze the cause of the leakage incident in cooperation with the Information Protection department, Personal information protection department, the IT department and professional outside organizations, etc. According to the results of the analysis, a security solution will be constructed additionally or the guidelines for personal information protection will be revised. If the personal information of more than 1,000 data subjects has been leaked out, the case must be reported to KISA without delay.

The laws related to Information Protection and personal information protection are being established and revised continuously. Therefore, relevant laws must be checked for any changes rather than one-time review to grasp the influence on the business of the company and, if necessary, reflect the changes to the Information Protection regulations of the company and make sure that the executives and staff members of the company observe relevant laws.

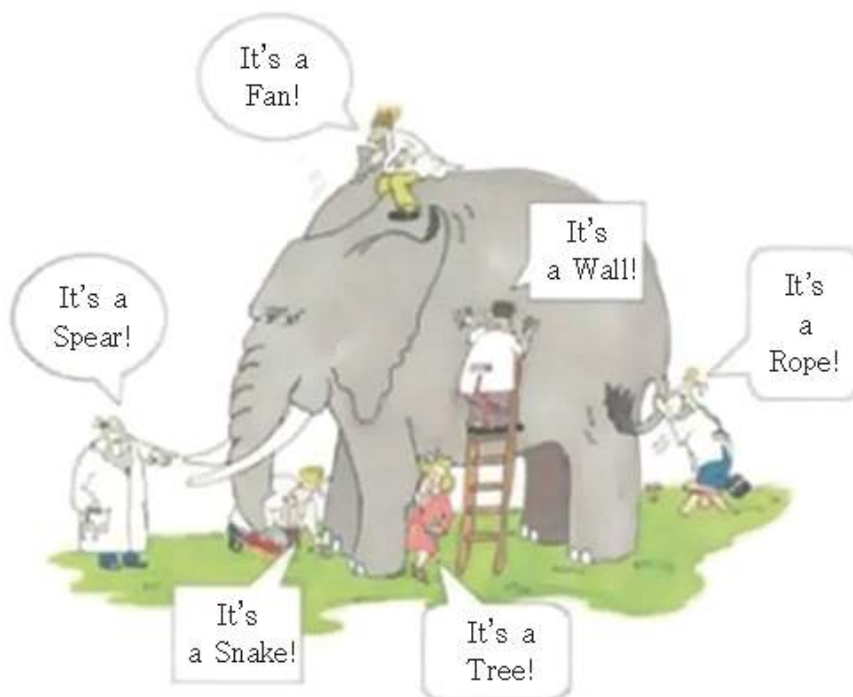
※ The establishment and revision of the laws related to Information Protection and personal information protection can be checked in the homepage of the National Law Information Center ([Http://www.law.go.kr](http://www.law.go.kr)).

2. The Security that CISO should know

Business entities these days are exposed to various kinds of security threats such as ransomware, GandCrab, malignant code, leakage of personal information, attempts to leak industrial secrets/trade secrets, attempts to forge homepage, infection with malignant codes, etc. Though business entities are responding to security threats with the latest technology, the attacking skills of outside security threats like hackers are also being upgraded.

The CISO needs to know the level of Information Protection of his/her organization accurately. The security level of the organization can be evaluated with various factors including the Information Protection capacity of the members of the organization, security architecture and performance of security architecture, and the level of awareness of the executives and staff members of the company. The level of weakness decided by consulting about Information Protection or the number of defects in the Information Protection management system are a part of the factors used for decision of the security level of the organization, but they are not decisive factors. As shown in Figure 2-2 below, it can be misunderstood that the result of analysis of the security in a part of the organization shows the level of the entire organization.

Figure 2-2 Fragmentary evaluation of the level of Information Protection



Source: HelloT News, June 6, 2018

When an Information Protection solution is introduced and installed, the effect of introduction of the solution must be explained clearly to the management. If it is explained that a certain Information Protection solution can prevent all security incidents once it is introduced, the management will probably be persuaded for the moment but from a long-term point of view it can be misunderstood that the Information Protection organization is not working effectively despite the high cost. The CISO must communicate with the management as a member of the management rather than as the highest person in the Information Protection department.

There are many factors which decide the level of Information Protection of an organization, but ultimately what is the most important is humans, i.e. the executives and staff members of the company. Therefore, it is necessary to change the level of awareness of the executives and staff members through various educational activities and raise the awareness of executives and staff members about Information Protection. By the way, such activities must not be one-time activities. It is necessary to establish the procedures that can create various programs which can raise the awareness of Information Protection and improve the awareness of executives and staff members continuously.

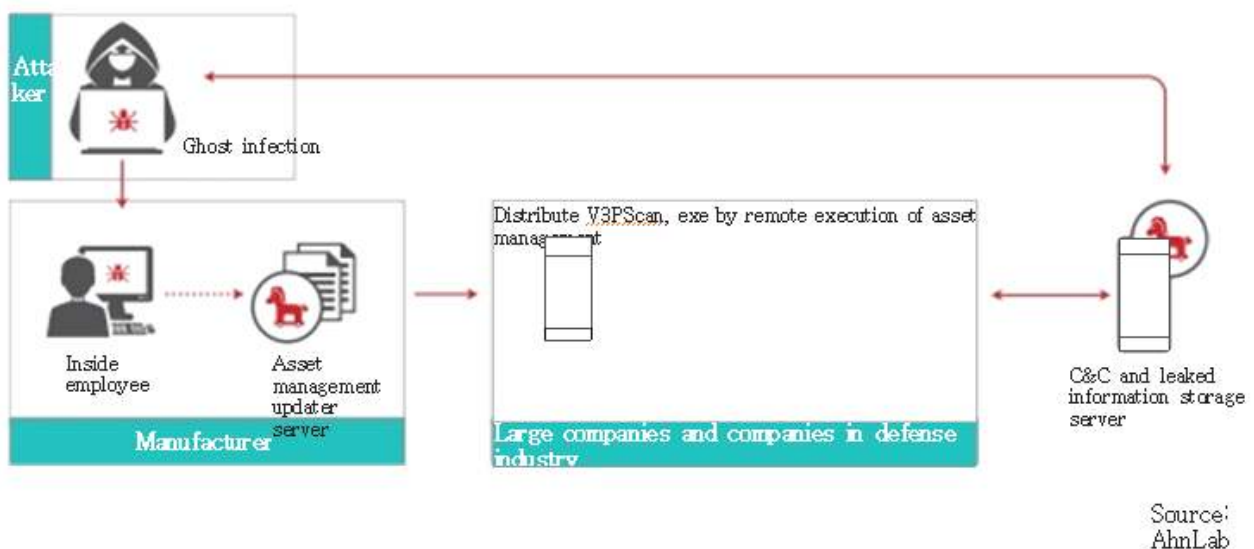
The CISO needs to analyze the cause of information infringement incidents of other companies and establish an Information Protection solution or revise the regulations on Information Protection, etc. in order to prevent a similar incident in the relevant organization. When establishing the Information Protection solution, it is necessary to use the internal Information Protection architecture or review the necessity and feasibility of introduction of the solution according to the mid- and long-term plan.

(1) Cases of security incident

Attack on supply chain security

The attack on supply chain security uses the method to hide a malignant code after hacking mainly the system of the development company, the update server, etc. because it is easier for the attacker to aim the one with relatively weaker security connected with the main target of attack than directly attacking a business entity or public agency that are equipped with a Defense-In-Depth system. When we receive the update file including a vaccine, etc. from the manufacturer, it is not easy to find out infection with a malignant code or forgery of the source program, and we have no choice but to trust and use the file sent from the manufacturer. If you are going to use a patch file, you had better not use the patch file right away and patch the file after checking its stability closely for a certain period of time. In addition, when patching is done from outside through remote access, it is necessary to use the exclusive line or the transmission segment encryption. Direct access to the internal network server or equipment must be restricted and it must be controlled to make the access through the Remote access server.

Figure 2-3 A case of supply chain attack



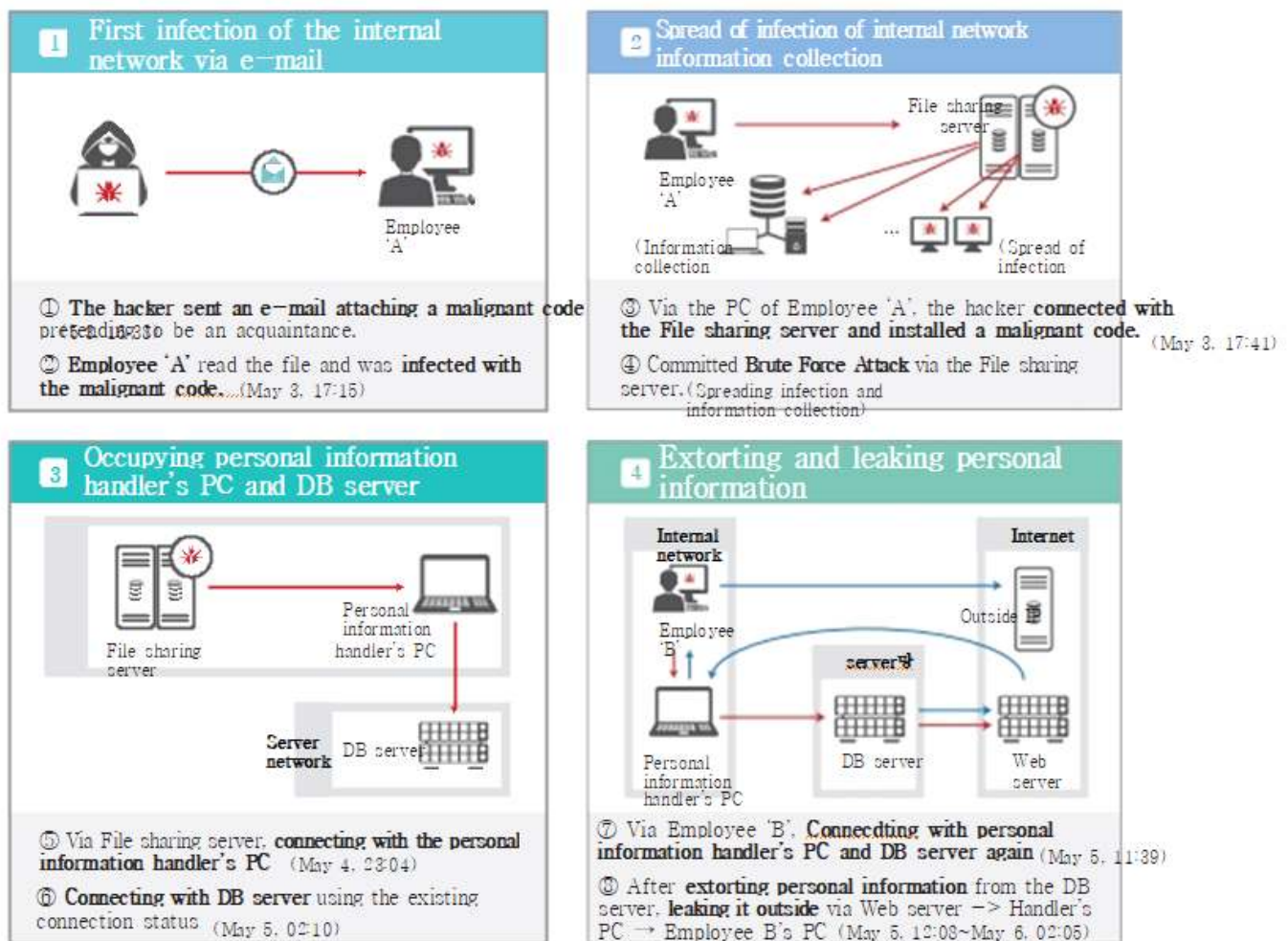
Cryptojacking

Cryptojacking is a type of cyber attack made on the victim by a hacker to mine cryptocurrency. The head of the Threat Intelligence Analysis Team of Check Point Korea Co., Ltd. said, "The problem is that Cryptojacking is being committed everywhere - in the web site, server, PC and mobile. About 55% of all organizations around the world are being affected." The simplest way to protect oneself against Cryptojacking is to install a Cryptojacking cutoff device, i.e. to add browser extension which blocks the list of domains that are related with Cryptojacking. The three extension functions especially made to cut off browse mining are AntiMiner, NoCoin, and MinerBlock.

Personal information leakage incident at "I" Company

It was found out that the personal information leakage incident at "I" Company was committed by a hacker who infected the PC of an inside employee of the company with a malignant code to obtain the DB account/password by collecting information. The hacker leaked out the personal information taken by connecting with the DB of the personal information processing system. There were weak points including non-application of the session timeout when connecting with the DB and insufficient network separation operation. Most companies which maintain ISMS-P certification set session timeout for connection with the administer page and the server/DB and separate the network for the personal information handler to prevent Internet access. The category of personal information handlers need to include not only the employees who can inquire/change/delete personal information by connecting with the personal information processing system but also the operators who connect with the server/DB/network equipment for safe operation of the service.

Figure 2-4 The result of analysis of the personal information leakage incident which occurred at "I" Company in 2016



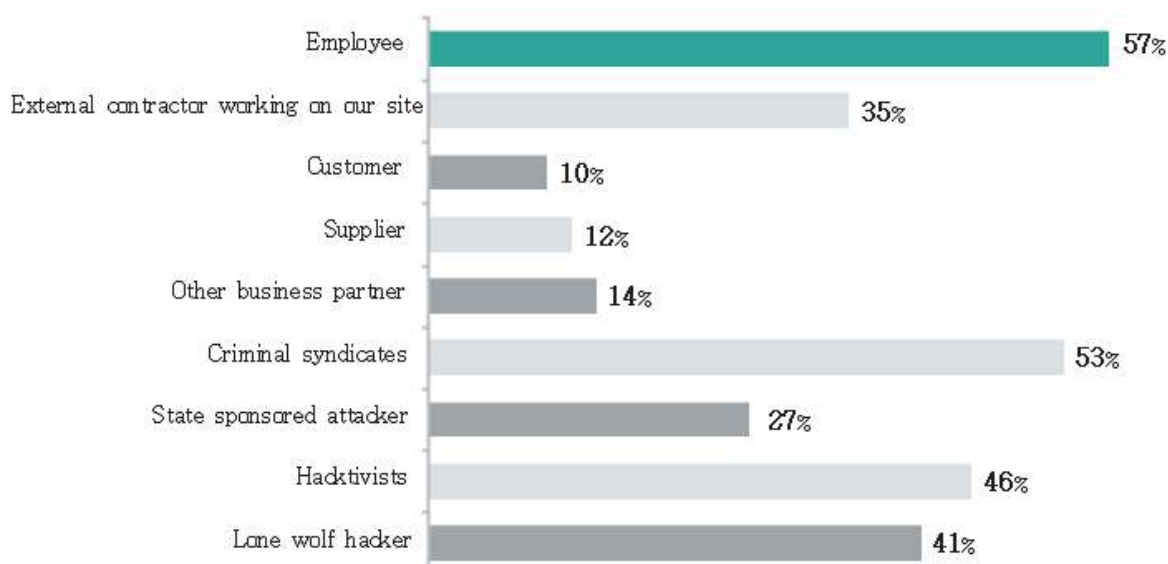
Source: Press release of Korea Communications Commission (Aug. 31, 2016)

Ransomware

Infection with “WannyCry” ransomware occurred throughout the world in May 2018. If a file was infected with WannyCry ransomware, the file was encrypted and a window popped up to demand \$300 in Bitcoin. While its damage in Korea was not so significant, some countries like the U.K. and Ukraine suffered serious damages due to infection of servers at government agencies.

The word ‘WannyCry’ has a dual meaning of Crypt and Cry, I.e. “Do You Wanna Cry?” and “Do You Wanna Crypt?” The name of the ransomware is “Wana Decrypt0r” meaning “Do you wanna decrypt the encrypted file? The U.S. National Security Agency (NSA) was blamed for the incident as the incident occurred by leakage of the Zero-Day weak points of NSA to a hacking group named ‘The Shadow Brokers’. The security patch for the weak points was provided from Mid March of 2017, but the office PCs not updated with the vaccine and firewall due to compatibility with the programs for working or the PCs with Windows XP without a security patch suffered from much damage. In Korea, even the backup data of Internet hosting companies for possible infection with ransomware was encrypted and some companies couldn’t recover the services completely despite payment of the money to the hacker. In order to protect the organization against ransomware, the operation system must be updated regularly and the information saved in the PC needs to be backed up periodically. According to the survey of EY, a global consulting company, 57% (including overlapped answers) of the respondents answered that “the principal agent for leakage if information is the executives and staff members.” It can be assumed that the executives and staff members may leak important information due to their mistakes or by outside temptation. Thus, it is necessary to not only establish a solution for detection and prevention of information leakage but also strengthen security capacity by raising the awareness of the executives and staff members.

Figure 2-5 Principal agent of information security incident



Source: EY GISS 2014



the CISO

Guidebook

Basic

III

Information Protection Regulation Establishment



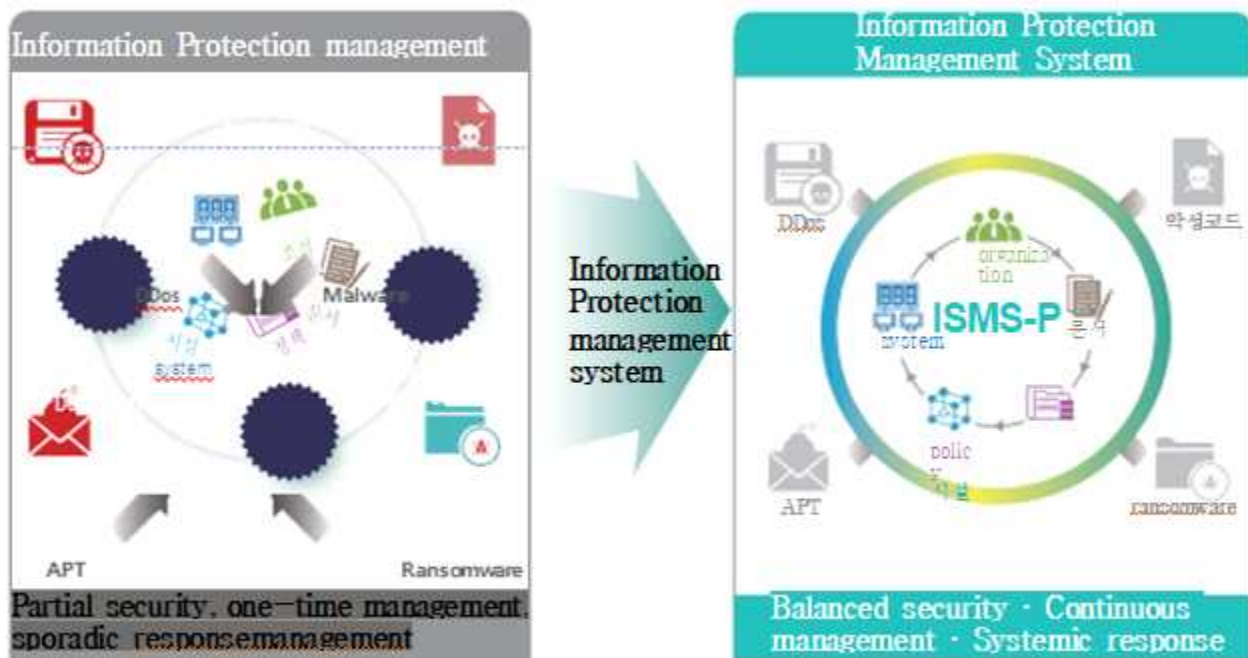
1. Overview of Information Protection Regulations
2. How to Prepare Information Protection Regulations
3. Cases of Information Security Regulations

1. Overview of Information Protection Regulations

The Information Protection Management system is a comprehensive management system that includes administrative, technical and physical protection measures to secure the safety and reliability of information and communications networks, and the overall organization in preparation for IT proliferation, paradigm change, and increase in cyber infringement. It means a systematic risk management system.

Establishment of information protection management system companies that do not respond temporarily to information security threats and partially perform security in areas that are needed immediately, so even if countermeasures are established for the same threat, it becomes difficult to respond to similar threats that have been modified. Therefore, the information protection management system for systematic and continuous response must be established.

Figure 3-1 Definition of Information Protection management system



Source: KISA

In order to continuously manage and respond systematically according to the information protection system, it is necessary to establish specified information protection policies/guidelines so that employees can conduct consistent information protection activities. If there are no security regulations such as documented information protection policies/guidelines, the level of information protection continues to decline as executives and employees perform information protection activities randomly and are not controlled or managed.

In addition, if the subject of execution is not clear, information protection activities are not normally performed or if there is a suspicion of an infringement it may take a long time or may not be analyzed.

It is difficult to say that the implementation of documented information protection policies/guidelines sufficiently prevents infringement or personal information leakage. However, the effectiveness of documentation reduces the scope of damage from infringement incidents or personal information leakage incident. In the event of an incident, it is possible to ensure prompt judgment and quick response. In order to sufficiently secure the effect of documentation, periodic and continuous information protection education should be provided to executives and staff members, and if training is necessary, periodic training should be provided so that the information protection activities to be performed by individuals can be internalized in their respective tasks.

Figure 3-2 Effect of Information Protection management system

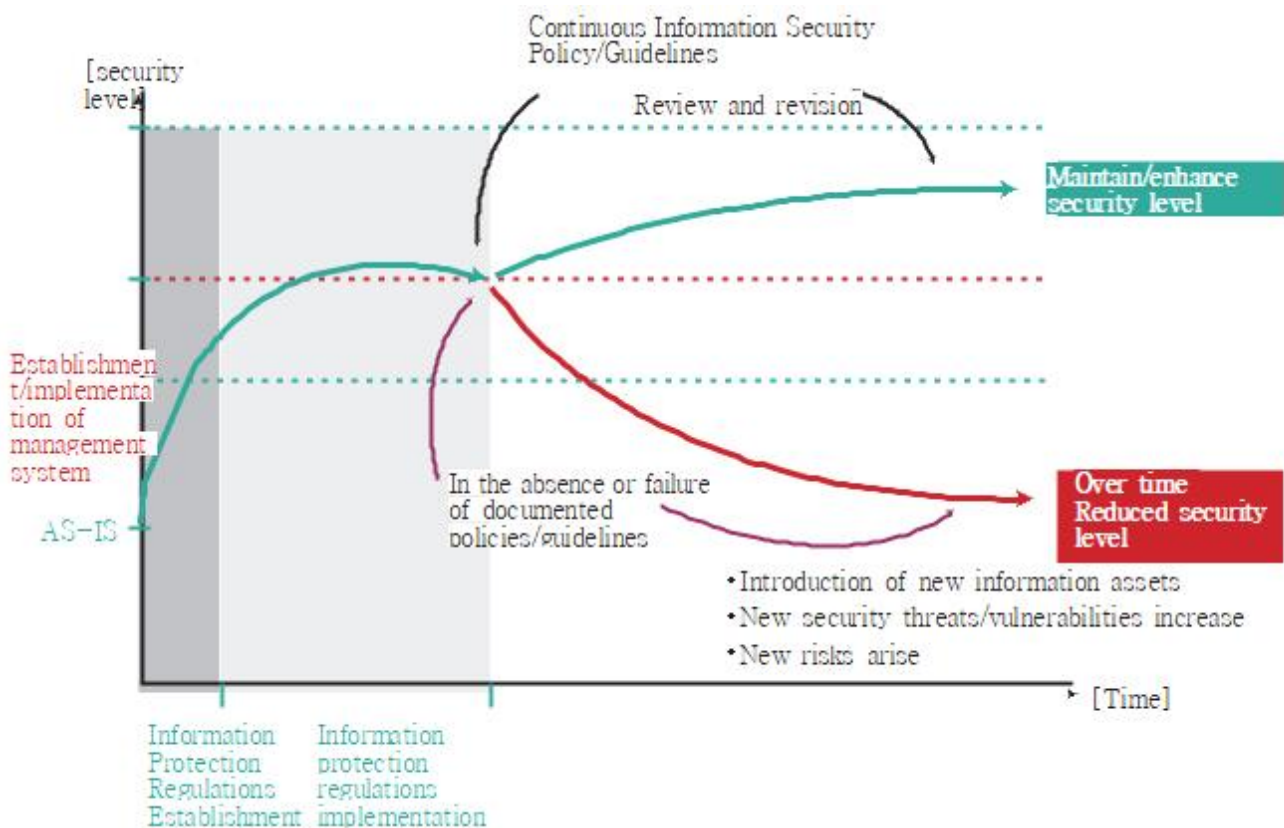


Figure 3-3 Information Protection system

The system for information protection regulations can be configured according to the system according to the company rules of each organization. Even if information protection regulations are established according to company rules, it is recommended to organize information protection policy documents, policies, guidelines, manuals/guides, etc.

The policy paper presents the highest level of goals, directions, and principles for management. Since the policy paper presents the principles of information protection, when writing sub-policies/guidelines, it is necessary to consider sufficiently to avoid violating the principles. If the establishment of internal policies/guidelines due to technological advancement cannot be followed, information protection procedures can be performed based on principles. If there are any significant changes significant change in business (new businessIf there is an addition or sale of business, etc.), it can be reviewed and revised.

The policy must be observed by employees in accordance with the principles of the policy paper which define specific matters to be done and reflect the organization's management philosophy. Management should formulate and document policies that include overall goals and directions for information protection, publish them to executives and employees, and control them to comply with the policies. In addition, management should fully explain the policy to members affected by the policy, perform necessary procedures to understand the intent of the policy, and apply it to not only internal employees but also employees of external partners. The policy isReview and need at least once a yearCity will be revised.

The guidelines set out specific and detailed methods for complying with the policy, and provide practical standards.In general, detailed areas such as guidelines for management of individual information assets, development and operation, applications, information asset management, risk assessment and management, and physical security are prescribed.

2. How to Prepare Information Protection Regulations

When establishing regulations such as information protection policies/guidelines, the organization's characteristics and IT/information security culture should be considered, and the following should be considered.

(1) It should reflect the regulatory or legal requirements of the parent organization.

The information protection policies/guidelines presented by the organization's parent organization (holding company, parent company, etc.) and legal requirements related to the business of the organization should be reflected. As personal information leakage incidents and personal information misuse incidents occur frequently, laws and administrative rules related to personal information protection are continuously strengthened.

After identifying laws to be enacted and amended, they must be reflected in internal information protection regulations.

(2) Other regulations should not prescribe the same content.

For example, if account and password management is reflected in the server/network/information protection system/DB/personal information processing system/application system security guidelines, respectively, if some of the provisions are revised, all the contents must be found and revised. When the password change cycle is changed from 180 days to 90 days, the password change cycle will remain the same as before, for the guidelines that are not revised. After stipulating in a specific guideline, the rest of the guideline should be established in a form that applies *mutatis mutandis* to the relevant provisions.

(3) Performing subject, method, and cycle should be specified.

There are various stakeholders related to compliance with information protection procedures such as information protection organizations, business department managers, developers, operators, employees, and employees of partner companies. Therefore, each provision of the policy/guideline must clearly define who will perform the execution subject to secure accountability and manage the information protection activities so that gray zones do not occur.

In each provision of the information protection policy/guideline, a cycle should be defined in consideration of legal requirements and the organization's information protection characteristics. If the cycle is not defined, it is difficult to secure an appropriate level of security because all information protection activities are observed once. By clearly defining the period (half year/quarter/month/weekly/day), information protection activities can be operated continuously.

(4) Approving authority for information protection regulations should be designated.

In the case of enacting or revising policy documents/policies, the relevant contents should be sufficiently discussed and reviewed with stakeholders (cooperation department and IT operation

department, etc.). This is because the management of policy documents/policies is performed by the information security department, but the implementation according to the provisions is performed by the stakeholders. In order for a policy document/policy to be effective within the organization, it must be reviewed and approved by management. The approval authority according to the information protection regulations should be decided in consideration of the size of the organization and company rules, but the policy document/policy is the management, the guidelines are the chief information security officer, the manual/standard/

The guide is recommended to be approved by the team leader of the working department.

(5) Use clear language.

Information Protection Policy/Guidelines The contents of each clause must be clearly written and expressed as "must be ~" rather than the meaning of choice such as "can be ~". In addition, the content of the provision should be so large that the interpretation does not change. The clue clause is to allow exceptions to the information protection control and should be given to a minimum, and when the control including the clue clause is mature enough, the clue clause must be deleted.

(6) Document the security activities currently being performed, not the best practices of other companies.

Since the best practices of other companies with a high level of information protection do not consider the organization's culture and business procedures, the requirements of the provisions do not fit the organization's environment and require excessive activities. So the law or Current business procedures should be documented to the extent that they do not deviate from the requirements of the higher authority.

Strong information protection policies/guidelines will continue to improve the level of information protection if employees comply well.

Organizations with a low level of information protection can raise the level of information protection by establishing and continually strengthening them so that employees can fully comply with them, rather than establishing strong information protection policies/guidelines.

(7) Information security audit result And third-party security incidents should be reviewed and revised if necessary.

If a large number of executives and employees are violating as a result of the company-wide information security audit, there are two aspects to review.

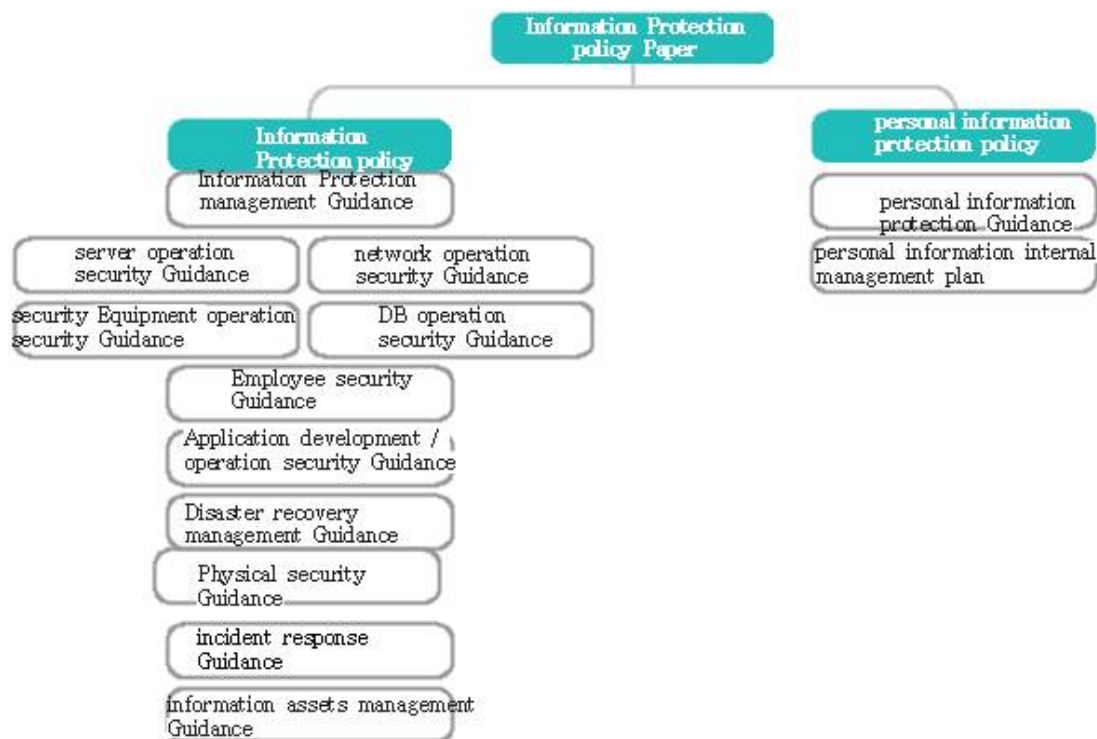
- Excessive information protection regulations Or data protection regulations are not missing
- Information protection regulations have been established, but are not observed due to lack of awareness

If information protection regulations are excessive or missing, information protection policies/guidelines should be established and revised contents should be trained. Even if there are information protection regulations, if they do not comply, they should be included in employee information protection training to raise awareness. In addition, if a third party infringement incident or personal information leakage incident occurs, the cause of the incident can be controlled in accordance with the information protection policy/guideline by referring to the cause analysis results whether there are provisions that should be reviewed.

3. Cases of Information Security Regulations

Information protection regulations must be established in terms of the organization. The type and content of the regulation are not standard defined, and it can be established in consideration of the characteristics of the organization.

Figure 3-4 Cases for Information Protection Regulation



Information protection management guidelines are required for the establishment and operation of the information protection management system, information protection organization, information protection education, information protection audit, and documentation, security procedures before/on work/when leaving internal employees, external contracts and outsiders. Includes regulations on security management, etc.

Server operation security guidelines are the introduction/installation of servers. City preliminary security review, security vulnerability check, account and password policy, Review access rights, set log. And regulations for analysis, access control, backup and recovery, and asset disposal.

(Security Guideline for Security Equipment Operation) Introduction/Installation of Information Protection System. City security review, rule set setting and management, account and password setting procedure, access authority review, log setting and analysis, removal of unnecessary services, backup and

Recovery, asset destruction, Firewall/IPS/DDoS/SSL VPN/IPSec VPN And regulations on operating regulations for terminal security solutions.

(DB Operation Security Guidelines) Introduction/Installation of DBMS City security review, account and password settings, encryption, access rights Review, log settings And regulations for analysis, backup and recovery, and asset disposal.

(Employee Security Guidelines) Account And password, PC payment and use, Internet and e-mail use, mobile device use, Use of software Includes regulations on city security procedures.

(Application development/operation security guidelines) Separation of development/operation, analysis of security requirements, definition of information security requirements, Account/password/authentication/log/access authority design, safe programming, outsourced development security, configuration management and operation Transfer, source check And regulations on vulnerability check, change and emergency change procedures.

(Disaster Recovery Management Guidelines) Disaster Recovery It includes regulations on organizational composition, business importance and impact analysis, classification according to business importance, RTO/RPO evaluation, disaster recovery plan establishment, disaster recovery plan training, and follow-up management.

(Physical Security Guidelines) Designation of security zones, work in control zones, cables And power line protection, access control, and asset transfer It includes regulations on control, office security, and image information processing equipment operation.

(Guidelines for Response to Infringement incidents) Organization of Infringement Incident Response Organizations And responsibility/role, definition of the severity of infringement incidents, analysis of signs of infringement incidents, reception of infringement incidents, reporting to external organizations of infringement incidents, investigation of infringement incidents, response to intrusion incidents, intrusion incident recovery, Includes rules for follow-up management, etc.

(Information asset management guidelines) Asset management procedure, asset identification And classification, asset importance assessment, asset introduction and change, Idle equipment management, asset disposal, asset class It includes provisions for individual protection measures.

(Privacy Guidelines) It stipulates procedures and methods to internally comply with administrative rules such as the Information and Communication Network Act and Personal Information Protection Act. The guidelines for personal information protection do not reflect the contents of the law in the same way, but reflect the practical contents of how to implement the contents of the law through internal business procedures and information protection systems. If the contents of the Personal Information Protection Act are reflected, the contents related to public institutions should not be reflected in the privacy guidelines.

(1) Information protection policy Paper

The information protection policy is a document that the top management presents to executives and employees the principles and directions for information protection include the willingness and support of top management.

Information Policy Protection Policy Paper

PaperVarious sophisticated and sophisticated threats with the advent of new technologies can seriously affect OOOO's information assets, which provide IT services. As a global leader, OOOO's efforts to provide safe and personalized services have made information protection activities an indispensable element, not an option. Therefore, all employees of OOOO thoroughly consider the loss of important information assets from security threats such as internal and external hacking and information leakage, delays and deterioration of work, and various legal, social, and ethical consequences. To prepare appropriate preparationYou have to do your best.

Accordingly, OOOO establishes and proclaims the following information protection principles.

- (1) Protect OOOO's information assets from illegal access and leakage.
- (2) Maintain the confidentiality, integrity and availability of OOOO's information assets.
- (3) OOOO complies with legal security requirements related to information protection.
- (4) All employees of OOOO recognize the importance of information protection, and are able to properly prevent, detect, and respond to incidents.Should be.
- (5) OOOO conducts periodic analysis, inspection, and audit of risks related to information protection.

OOOO invests the time and resources necessary to comply with this information protection policy, and organize and operate an organization that manages information protection. Information protection cannot be carried out only by a specific management organization, and above all, it requires the participation and responsibility of all employees. Therefore, all employees must do their best to understand and comply with the declared policy with an awareness of the importance of information protection and with continued interest.

20XX. 00

Hong Gil-dong, CEO of OOOO Co., Ltd.

(2) Information asset management protection guidelines measured by asset class

Information asset management guidelines should establish information asset classification standards and materiality evaluation standards, and establish protection measures for each asset class for assets evaluated according to the standards.

If the same security measures are applied to all information assets and can be managed at a high level, protection measures for each asset class are not necessary. If there is a limit to the budget that can be invested in information protection or there are not many managers, assets with high importance should be protected first according to the protection measures for each asset class. If there is no protection standard for each asset class, security control may be weakened due to the omission of protection measures in some of the important assets.

The following is the protection measures for each asset class. This is an example of protection measures for middle server assets. When classifying information assets, it is difficult to differentiate the different protection measures for each class. It is recommended to classify.

Chapter 00 Protection Measures for Each Class of Assets

Article XX (Protection Measures by Server Class)

① The protection measures for the 1st class server are as follows.

1. It is installed in the internal network, a separate zone is configured and operated, and access control is performed through a firewall.
2. It must be operated in a server room where reinforced access control such as card key and fingerprint recognition is applied.
3. User authentication method is based on knowledge, ownership, and biometrics. A method that uses two of these factors should be applied.
4. To prepare for security incidents and fatal failures, monitoring should be performed at all times.
5. To prevent security incidents, the server person in charge should conduct a quarterly vulnerability inspection.
6. No administrator authority should be granted other than the server person in charge.
7. Control should be applied to users and IPs that can be accessed using an access control function or an access control system.

② The protection measures for the 2nd class server are as follows.

1. It must be installed and operated in the internal network.
2. It must be operated in a server room where access control such as card key is applied.
3. User authentication method should apply authentication using ID/PW.
4. In order to prevent security incidents, the server person in charge should conduct vulnerability inspections once a half year.
5. Controls must be applied to users and IPs that can be accessed using the access control function.

③ The protection measures for Level 3 servers are as follows.

1. It must be installed and operated in the internal network.
2. It must be operated in a server room where access control such as card key is applied.
3. User authentication method should apply authentication using ID/PW.
4. In order to prevent security incidents, the server person in charge should perform vulnerability inspection once a year.
5. Controls must be applied to users and IPs that can be accessed using the access control function.

(3) Security guidelines for employees

The employee security guidelines include regulations on account and password, PC payment and use, Internet and e-mail use, mobile device use, and security procedures when using software. PC/terminal should be used only when officially paid by the company, and personal PC should not be brought in. E-mail should only be used with the company's official mail system, and commercial e-mail provided through the Internet should be controlled not to be used. In the case of software, the security solution installed on the terminal is installed and paid in advance when the PC is paid, and software that the company has licenses must be used.

The following is an example of regulations on the account and password of employees. In the case of passwords, "Standards for technical and administrative protection of personal information" in the Information and Communication Network Act or "measures to ensure the safety of personal information in the Personal Information Protection Act Standards" should be observed.

Article XX (creation, change, deletion of user account)

① The procedure for creating a user account is as follows

1. The account applicant fills out the "User Account Application" and requests the system manager after obtaining approval from the department manager.
2. After receiving the request, the system person in charge creates an account and grants the requested authority, and the information protection person in charge should periodically review the appropriateness of the granted authority.
3. Groupware accounts are created by the person in charge of the HR system after joining the company, granting access rights according to departments and roles, and the person in charge of information security should periodically review the appropriateness of the authorization procedure.

② User account change and deletion procedures are as follows.

1. When a job change or resignation occurs, the head of the department receives a "user account application" from the party and submits it to the system manager.
2. The system manager changes the access rights of the account that requested the change of job, and the resigned account is deleted immediately after leaving the company.
3. If the relevant department requests that the resignation's account is necessary, it can be maintained for up to one year with the approval of the chief information protection officer.

Article XX (Password Creation and Management)

- ① Employees who are notified of account creation must log in immediately and change their initial password.
- ② For executives and employees, the password setting must include at least 8 English letters, numbers, and special characters.
- ③ Employees must change their password every 90 days. However, the password of the account that can directly affect the operation of the system can be excluded if it is approved by the chief information protection officer.
- ④ The system manager must set the previous password (3 times) not to be reused.
- ⑤ The system manager must mask the password when it is displayed on the screen.
- ⑥ Employees must change the password immediately if the password is exposed.
- ⑦ The system person in charge must notify the employee through SMS when sending the initialized password.
- ⑧ When setting the password, the system person in charge must set the password so that it cannot use the password that does not correspond to each of the following items.

1. Password same as ID
2. Abbreviations or words related to company name, department name, service name, etc.
3. Words registered in the dictionary
4. Password with 3 or more consecutive same letters or numbers
5. A password consisting of letters or numbers
6. Periodic characters (abcd, 1234, etc.) and consecutive arrangements on the keyboard (asdf, qwerty, etc.)
7. Password less than 8 characters

Article XX (User Rights Management)

- ① When granting authority to a user, the system manager must give it the minimum authority necessary to perform the task.
- ② The system manager can limit or withdraw the user's authority to misuse or abuse the information system.
- ③ After reviewing the access rights, the system manager locks accounts that have not been used for 3 months or longer, and deletes accounts that have not been requested for reuse for 3 months.

(4) Disaster Recovery Management Guidelines

Securing continuity of core business, IT services, and information systems in the event of a disaster define the necessary procedures for this. Identify core tasks and IT services based on disaster recovery management guidelines, determine recovery priorities through business impact analysis, recovery target time (RTO) according to recovery priority, recovery target point (RPO), training plan A disaster recovery plan including, etc. should be established. The disaster recovery plan should be revised annually after training according to the training results.

Article XX (evaluation of business importance)

- ① The person in charge of disaster recovery identifies disasters that may damage IT service and business continuity and Impact should be analyzed.
- ② The person in charge of disaster recovery should review the assessment of the importance of the work every year, and may request support from the system manager and the person in charge of the field during the review.
- ③ The person in charge of disaster recovery defines the recovery target point (RPO) and the recovery target time (RTO) through consultation with the person in charge in the field. It must be approved by the person in charge of disaster recovery.

Article XX (Establishment of Disaster Recovery Plan)

- ① The person in charge of disaster recovery must prepare a disaster recovery plan and obtain approval from the person in charge of disaster recovery in order to minimize business disruption due to disasters such as fire, earthquake, power outage, building collapse, and system interruption.
- ② The person in charge of disaster recovery must include the following items when establishing a disaster recovery plan.
 1. IT service (task) identification
 2. Prioritizing recovery of IT services
 3. Recovery Point Objective (RPO) of IT service
 4. Recovery Time Objective (RTO) of IT service
 5. List related IT resources and facilities
- ③ The person in charge of disaster recovery must include the following in the disaster recovery form.
 1. Organization and operating procedures in normal/disaster
 2. Find out the situation and write notification/dissemination procedures
 3. Mock training
 4. Maintenance
- ④ The person in charge of disaster recovery must provide priorities for emergency transported goods by preparing instructions for transport in case of a disaster.
- ⑤ The person in charge of disaster recovery shall establish emergency operation procedures and recovery procedures for recovery in the event of a disaster in consultation with the system person in charge, and provide training to executives and employees.



the CISO

Guidebook

Basic

IV

Raising Awareness of Employees



6. Prolog
7. Information Protection ... Why is it important?
8. Measures to Raise Awareness of Information Protection;
Understanding the basic concepts and steps
9. Measures of Raise Awareness of Information Protection;
Step by step and specific measures
10. Information Security Education Plan;
To Remind Employees of Information Security
11. Security Culture Settlement Plan;
Qualification of Security indicators
12. Epilog

1. Prologue

(1) An era beyond security technology; The era of legalization of security

When discussing the information security domain of a company, it is generally considered that administrative security, technical security, and physical security are separated by etc. The administrative security referred to here can be said to be a security that establishes and applies security procedures and checklists to be applied centering on the business processes handled within the enterprise. And it can be said that technical security is a technical means applied to protect many technical tools and equipment introduced/used for business processing of a company. On the other hand, physical security is applied to ensure that only authorized persons access the company and its facilities, and to protect the company and its facilities. Security I can do it.

From the perspective of this classification method, in the past, the central axis of corporate information security was technical rather than administrative security. It can be said that it was in security. This is because most of the methods of stealing corporate information, including customer information, used technical means. As a result, this It also served as an opportunity to strengthen security.

On the other hand, since the Personal Information Protection Act was enacted in 2011, various laws and procedures related to the protection of corporate customer information have entered the administrative security domain of the enterprise. In particular, the "Personal Information Protection Act" and the "Information and Communication Network Utilization Promotion and Information Protection Act" (hereinafter referred to as the "Information and Communication Network Act") and various guidelines and guidelines derived from these laws must be observed in the current era of corporate information security. Has become an essential law and guideline. This is because many companies currently use terms such as "security compliance" in their duties when hiring employees in the information security department. It can be said that corporate security has evolved beyond the 'technicalization of security' era to the "legalization of security" as the process has passed. Due to this, individuals, companies, organizations, and public institutions that can be free from laws related to information security. Even if there is no, it is not an exaggeration to say that the times have arrived.

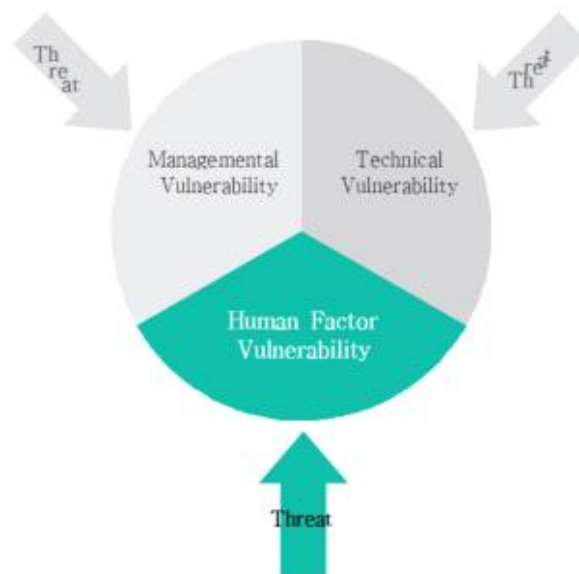
(2) The contact surface of the recently focused security threats; Human Factor

Information security There can be no perfect security. This is because attackers always develop new attack techniques and dig into the most vulnerable areas. In other words, just because you defend against today's attack doesn't mean you can defend even tomorrow's attack. As if it proves this, the latest security

Threats reduce administrative and technical security. It is consistently occurring in areas that are bypassed at once. That representative example is Ransomware.

In terms of information security In view, the biggest characteristic of ransomware is that it is the easiest and fastest way to bypass the existing "administrative security" and "technical security". This is possible because it is an attack that targets employees already within the administrative and technical security areas, that is, "people", and more precisely, uses', people's thoughts as a bridgehead. In view of the characteristics of such ransomware, it can be said that security threats through the "people's thinking area" that could not be covered by the technical or administrative security areas from the existing security areas are increasing. Therefore, from the perspective of an information security expert who is in charge of corporate information security in the present time, it is called "Human Factor" in the existing information security area. To overlook the strengthening of security for the "people's thinking area" It can be said that it has become impossible.

Figure 4-1 The contact surface of the emerging security threats



(3) Real examples of attacks targeting Human Factor vulnerabilities: Ransomware

According to the security issue data and security seminar presentation data of Ahn Cheolsoo Research Institute in 2017, from 2013 to 2015, there were 9 types of ransomware that appeared during the year, but in 2016 it increased to 163 types. This is how an increase of 18 times, where the important thing to know is that the attack vector of the attacker has changed. In the past, attacks were conducted by infiltrating technical security controls, but in recent years, attacks were conducted through the thoughts of employees (ie, people) within the technical security control area has changed.

Figure 4-2 Conversion of Attack Vector



This change in attack vector through human thought is a very cost-effective situation from the point of view of an attacker, while it is a very threatening situation from the point of view of corporate information security. This is because the attacker not only does not spend the time and effort necessary to overcome the technical security control, but also can secure the information or value held by the company through the thoughts of employees within the technical security control area. This situation is inevitably a big threat as it acts as a burden on corporate information security.

Unfortunately, these threats have been increasing since 2015. It is increasing further. Korea Ransomware Infringement Response Center According to data, the number of domestic ransomware damage in 2018 compared to 2015. It can be seen that the amount of ransomware damage increased by about 12 times, and in proportion to this, about 13 times.

Figure 4-3 Domestic ransomware damage cases and damage scale



Most of these ransomware are infected through the "website", but they are also infected through the "company email" or "P2P site". From an information security perspective, In the case of a "web site" or a "P2P site", it is possible to technically block access to the site by using information assets within the company. However, in the case of "company e-mail", considering that it is necessary to continuously

send e-mails inside or outside the company, access to company e-mails is required to prevent ransomware infection. Blocking technically is an inappropriate security measure.

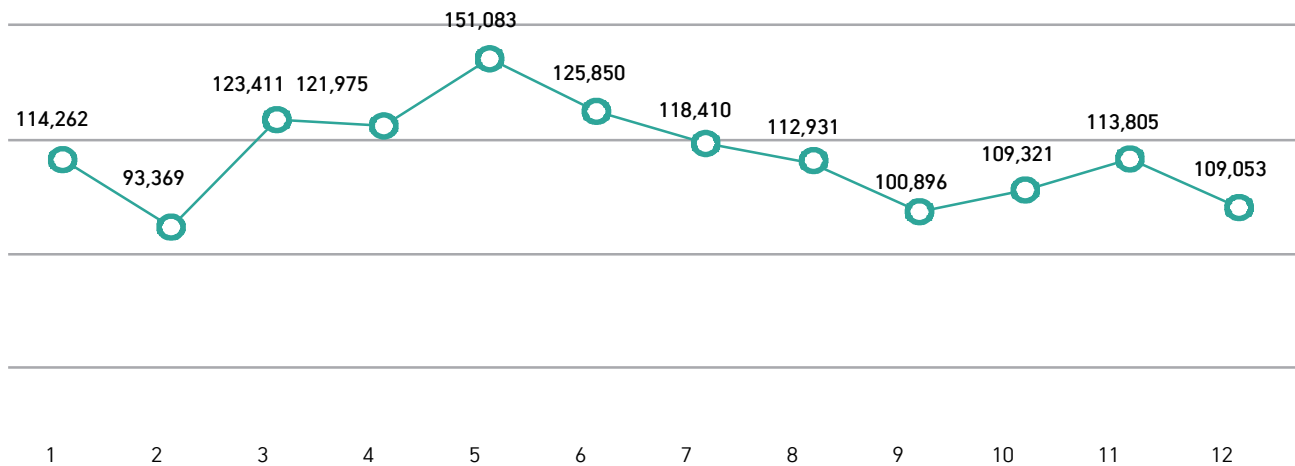
However, I think the attacker is very aware of this situation. This is because, in recent years, ransomware attacks via corporate email are evolving. Emails containing ransomware malware, for example, emails that utilize tensions between the two Koreas, emails for image copyright infringement, and traffic penalty bills. Such are the emails for 'Courier Delivery', 'Customer VoC' emails, and 'Defendant Summons' emails. In particular, looking at the attack method in which an e-mail containing ransomware malicious code is sent as an e-mail addressed to employees of the company's human resources department with the subject of 'Joining Application', it can be seen that the attacker already knows information about the target company. In addition, recently, ransomware malware has been planted in emails related to 'year-end settlement' in accordance with the year-end settlement season of office workers.

(4) Nightmare Scenario: What if you get ransomware?

According to the data of EST SECURITY published as an article through security news, East Security is 2018 About 1.4 million ransomware attacks were blocked during the year, which can be seen as blocking more than 100,000 ransomware attacks on average every month.

Figure 4-4 Monthly ransomware blocking statistics in 2018

(Unit: case)



Source: East Security

But, if there is about 100,000 per month, what would happen to companies if they couldn't stop one or more than one ransomware attacks? In particular, some of the employees who received ransomware via e-mails that are not technically inadequate to block access, and who are not aware of information security What if you click on an attachment or a via link in an email?

First of all, it is obvious that a business PC that clicks an attachment or a via link in an email containing ransomware will be infected with ransomware. However, since recent ransomware is not simply aiming at one business PC, it can infect not only servers or databases operated in the company, all business PCs, but also shared files can be used for business purposes with the approval of the information security department.

If infected by ransomware, the situation does not end by itself, but infection itself begins a new phase. In other words, in order to secure the password of a device or file infected with ransomware, you have to pay a certain amount. Typically, a PC is estimated that it costs about 3 million won per month. However, given the total damage to which a company will suffer, these costs are only the tip of the iceberg. This is because, in addition to paying the cost, more damage than that constitutes the body of the iceberg. Based on these contents, a possible scenario is as follows.

Nightmare scenario

◆ Situation

Recently, an incident occurred in which a startup company that provides quite promising web/app-based services is infected with ransomware. This startup company is a company with annual sales of about 100 billion won, operates 263 business PCs, and the average monthly users using the company's service reaches about 1 million. The company was applying necessary technical security measures to maintain safe service and protect customer's personal information. As a result of investigating the cause of the ransomware infection, an experienced employee who recently transferred from another company to this startup company clicked/executed the attachment in the company email, and via the work PC of this experienced employee Company-wide work. It was confirmed that the PC was infected with ransomware.

Figure 4-5 Loss cost for ransomware (example)

Computer Ransom cost: 789,000,000 won = about 3 million won × 263 computers

+

Other loss costs to consider

Loss due to non-use of PC(Existing daily, weekly, monthly sales)
Brand value damage(At least about 1% of annual sales)
Loss of market share(At least about 1% of annual sales)
User churn(At least 10% of average monthly users)
Infrastructure damage recovery and supplementary measures(PC repurchase, information recollection, work process rebuild, etc.)
Customer Compensation Fees and Legal Fees

◆ Tip of the iceberg

In general, the ransom for ransomware is reported to be about 3 million won per work PC, so the cost that this company has to pay to the attacker is 3 million won X 263 work PCs = 789 million won. Considering that this company is a company with annual sales of about 100 billion won, it might be considered a modest cost to ransomware of 780 million won. But this ransom, which is important here, is just a start. It is excessive and is only one part of the total damage, the tip of the iceberg.

◆ Iceberg torso

- Loss due to non-use of work PC
263 business PCs required for business processing and customer service and the information stored therein are incurred, resulting in loss of use. And these loss costs increase in proportion to the passage of time (eg daily, weekly, monthly, quarterly, semiannual, etc.).
- Service brand value damage
The brand value of the services created and built by this company is damaged. Of the annual sales Even 1% calculation would result in a loss of up to 1 billion won.
- Loss of market share
The value of a company's existence is profit creation, and market share is inevitably important for this profit creation. However, if a company that provides web/app-based services is infected with ransomware, it will naturally lose some of its existing market share. Calculating the rate of loss of market share by 1% of annual sales results in a loss of 1 billion won.

Via Human Factor vulnerability, an attack that shakes people's thoughts...
How do you defend yourself?

What should be the first consideration when building a defense against attacks that shake people's thoughts through the vulnerability of Human Factor like ransomware? It is, of course, the thoughts of the members who make up the company, which is the waypoint of the attack, or "people's thoughts." In particular, in the current situation where there are no office workers who can be free from information security related laws, reviewing the degree to which corporate members perceive the importance of information security is in order to supplement the Human Factor vulnerability.

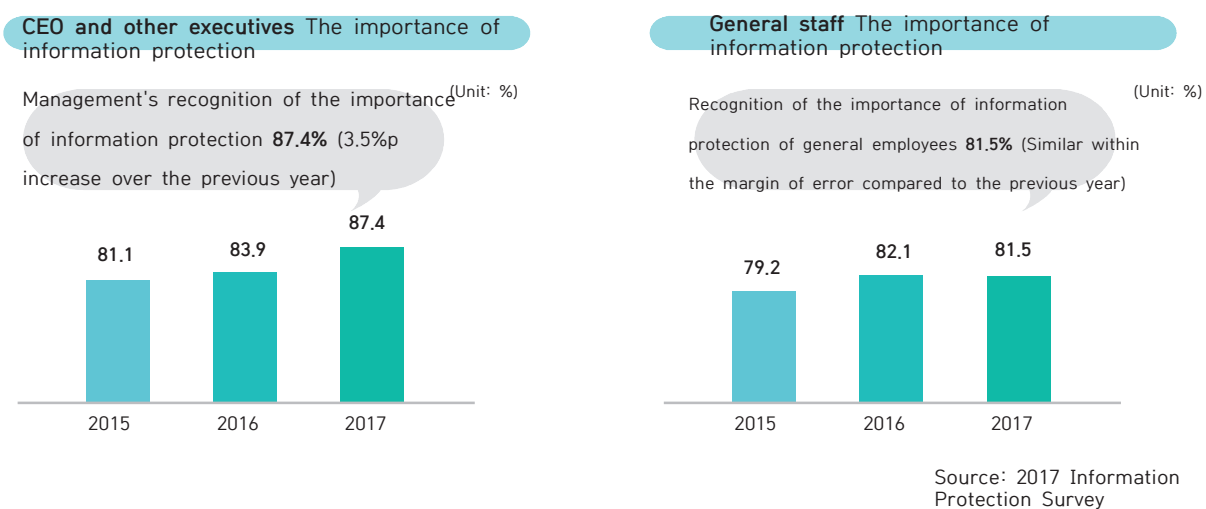
It can be used as a very important criterion.

2. Information Protection... Why is it important?

(1) Current status of employees' awareness of information protection

According to the 「2017 Information Security Survey」 planned by the Ministry of Science and ICT and conducted by the Korea Internet & Security Agency, the CEO And the management's perception of the importance of information protection 87.4% was found, and 81.5% of general employees perception of the importance of information protection.”.

Figure 4-6 Level of awareness of the importance of information protection by corporate members



(2) The reality in which people are the threat of information protection

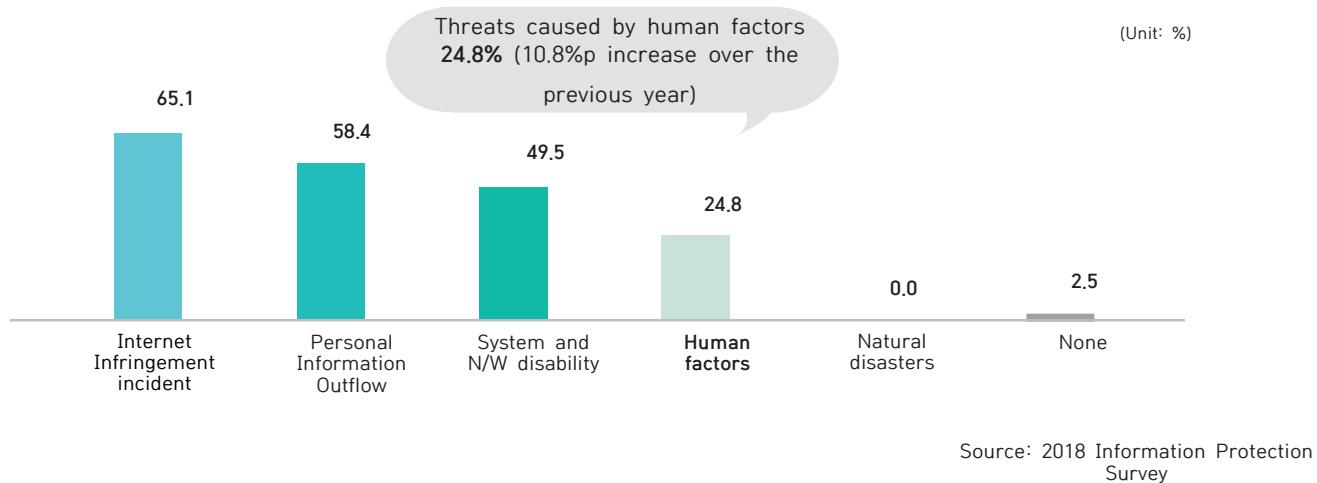
1) Number shown

How much of a company's members, that is, people, can be a threat to information security? The factors that threaten the information security system established and applied administratively and technically are considerably more than expected, but it is necessary to classify each factor into the largest category and to explicitly confirm each ratio. The Korea Internet & Security Agency released the “2018 Information Security Survey” the following year when the “Information Security Survey 2017”, which was previously examined, was announced. III) System and N/W disability iv) Human factors v) Natural disasters.

Looking at the ratio of threat factors by each category, i) Internet infringement incidents: 65.1% ii) Personal information leakage: 58.4% iii) System And N/W disability: 49.5% iv) Human factors: 24.8%. Looking at the ratio of human factors as a threat to information protection among these threat factors, it can be seen that 14% in 2017 but 24.8% in 2018. This is an increase of 10.8% compared to

the previous year (14%), which can be interpreted as a growing empirical or predictive perception that the information protection system may be threatened by people among corporate members.

Figure 4-7 Information Security Threat Factor Analysis



2) Hidden numbers

As can be seen in <Figure 4-7>, it is by no means a small percentage that the number of human factors among the threat factors of information security is 24.8%. However, in fact, there is another human factor hidden in <Figure 4-7>. It is hidden under the category “Personal Information Leakage (58.4%)”. Looking at the “factors of personal information leakage”, i) external hacking ii) leakage of management errors iii) outflow of insider intention iv) leakage of outsourced employees are working as a detailed factor. “Intentional outflow of insiders” and “outflow of outsourced employees” can also be attributed to human factors.

The proportion of human factors among the threat factors for information protection hidden in the “Personal Information Leakage Factors” also occupies a significant proportion. 73.6% of “management errors”, 33.4% of “intentional leakage of insiders”, and “outsourcing of employees” accounts for 11.7%.

Figure 4-8 Human factors hidden in personal information leakage factors



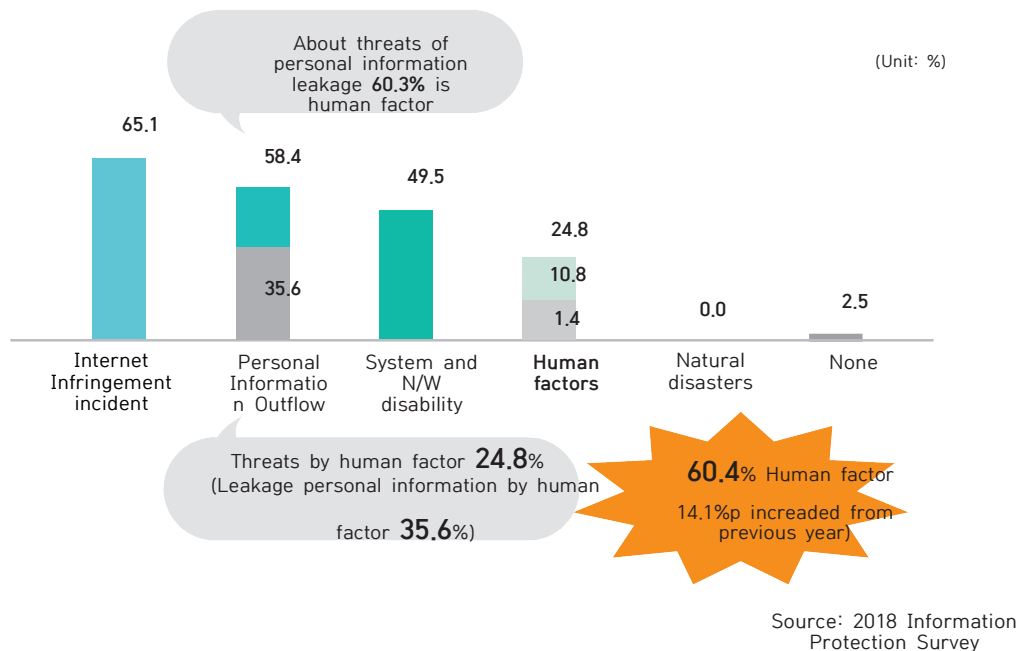
Source: 2018 Information Protection Survey

Information protection threats hidden inside the entire “Personal Information Leakage Factors “. The proportion of human factors reaches a whopping 60.3%. In other words, 35.6% or 60.3% of “personal information leakage”, which accounts for 58.4% of information security threats, can also be interpreted as a human factor among information security threats.

3) A number plus the meaning of the lines

As a result, it can be seen that another human factor (35.6%) that was not included in the existing human factor (24.8%) among the threat factors for information protection was hidden within the “personal information leakage factor”. Therefore, when determining the proportion of human factors among the threat factors for information protection, hide in the existing human factors (24.8%) and “personal information leakage factors”. It should be judged by adding the human factors (35.6%).

Figure 4-9 Threats to information security by adding the number of linesRatio of human factors

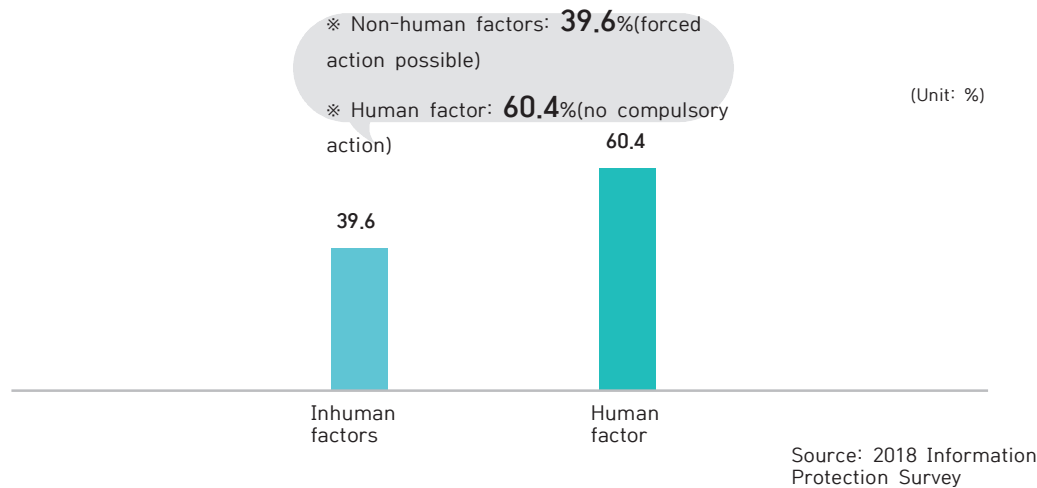


In light of this, the ratio of human factors, which is the ratio of “experiential or predictive perception that the information protection system may be threatened by people” among the threat factors of information security, is 60.4%, which is 14.1% compared to the previous year.

(3) Why information protection awareness is important

1) More than half of the threats to information security; ‘Person’

Surveyed by Korea Internet & Security Agency, the data security threat factors are classified into “human factors” and “non-human factors” by adding the meaning between lines to the results of the “2018 Information Security Survey”, the human factor is 60.4%, so the non-human factor corresponds to 39.6%. Based on this ratio, more than half of the threats to information security come from humans.

Figure 4-10 Ratio of non-human and human factors

Should not be overlooked in <Figure 4-10> There are two characteristics that cannot be done: i) the ratio of human factors is much higher than that of non-human factors ii) for the non-human factors, compulsory measures are possible through technical security control, whereas for the human factors, compulsory measures are impossible. Point. Considering these characteristics, it is possible to use the security pledge (so-called 'NDA'), which is written at the time of entering or leaving the company, but even so, considering the aspect of the attack that passes through the human thinking area, the security pledge is used to describe the human thinking area.

2) Weakest link ; “The area of human thinking”

In consideration of raising awareness of information security, the premise that “people's thoughts can change at any time” is a considerable burden. This is because even for departments or employees with a high level of information protection awareness at the moment, the level of information protection awareness may change at any time depending on future department/business changes or business issues. After all, in the information security system of a company, that is, employees, The thought domain is bound to be the weakest link.

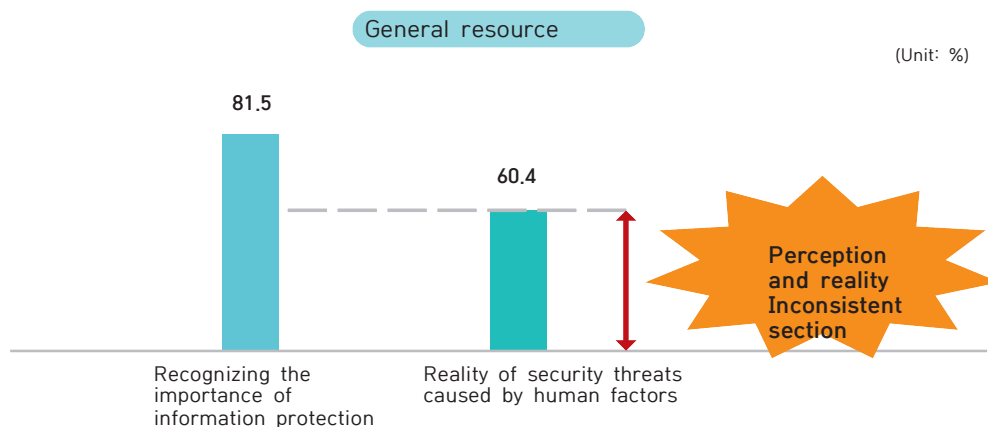
(4) The cycle of ironic phenomena

In the process of corporate activities in the era of legalization of security, the information protection system prescribed by the law must be established and applied. Therefore, the administrative security system and technical protection measures based on the law are essential and minimal information security systems. Therefore, in a legal-based information security system, "observance of the law" should lead to "maintenance of the information security system", which can be done with a natural logical structure. However, there is a phenomenon that breaks down the natural logical structure in an instant. In particular, this phenomenon is remarkable in the members of the company, that is, "the area of human thinking". Looking at it is as follows.

1) Discrepancy between perception and reality

As seen previously from this <Figure 4-6>, 81.5% of general employees believe that information protection is important. And the rate of recognition of the importance of information protection is also increasing every year. However, as shown in <Figure 4-10>, as many as 60.4% of the threat factors for information protection showed that human factors, that is, people, could shake the information security system. This contradictory situation can be said to be "a discrepancy between perception and reality". In other words, despite the fact that information protection is considered important, which means it's not being well kept.

Figure 4-11 Difference between perception and reality



2) Technical security bypass

In a company in which an information security system with administrative controls and technical protection measures applied, there are two ways in which employees perform their work. In other words, it is safe because it complies with the ① information security system, but it is a way that is somewhat inconvenient for employees to perform their work, and ② it is dangerous because it does not comply with the information security system, but it is a convenient way for the employee to perform the work. In the area of human thinking, we are contemplating which method to choose from

these two methods, but unfortunately, there seems to be a great tendency to choose a "dangerous but convenient method". In other words, it can be said that in the area of human thinking, there is a higher possibility of choosing a "dangerous but convenient method" rather than a "safe but uncomfortable method". Most companies operate technical protection measures to prepare for external intrusion or internal leakage. However, attempts to bypass or actually circumvent these technical protection measures among members of the company are the result of choosing the "dangerous but convenient method". It can be said to be an action that appears.

3) Resistance to management security

Companies operating an information security system basically apply administrative security controls called "information security policies" to all employees. Therefore, company-wide employees may have to comply with various procedures in accordance with the information security policy in the process of performing their work and, if necessary, undergo approval and review by the information security department. Through this series of processes, administrative security controls function within the enterprise. It becomes. However, the members who complain about these administrative security controls with the wrong view will be. In particular, these members have a negative view on the administrative security control procedures they must comply with. For example, if the information security department reviews the security for a specific system development or business plan and says that the development environment or business process needs to be changed, "I can't work because of information security" or "Do you mean to work? Are you saying dry?", "Will the information security department be responsible if development or work doesn't work?" and start complaining and complaining about information security around them. In other words, as they think and judge only from their own work point of view, they perceive information security, especially administrative security control, as an obstacle that interferes with the performance of their work to resist.

There are two facts that members who resist security controls with negative perceptions do not know or admit. The first is that security has been legalized. That is, for each company. It is not necessary to do it or not, but it is the administrative and technical security control that must be observed within the minimum necessary range. The second is the fact that the information security department also performs its own duties. In other words, the fact that the security review from the perspective of information security in the development planning or business planning stage and performing all tasks related to information security is not to interfere with the work of other departments, but to perform the unique work of the information security department.

As is well known, when boarding a Seoul city bus from January 2018, the safety of other passengers. For this reason, boarding with hot drinks is prohibited. In this case, the bus driver may refuse boarding, and passengers who eat food on the bus may be asked to get off. The basis for such safety control is the Seoul Metropolitan City Ordinance. Based on these Seoul Metropolitan Ordinances, few

passengers resist bus drivers when they refuse boarding for passengers who want to board the bus with hot beverages or request alighting for passengers who eat food on the bus. Similarly, the Road Traffic Act prohibits unauthorized crossing of roads for the safety of pedestrians and drivers. In addition, traffic police officers may impose penalties for pedestrians who cross the street in violation of these regulations. Under such circumstances, pedestrians who cross the street rarely resist traffic police officers.

But ironically, the legalized information security systemAs a result, the information security department or the information security person in charge of security work often resists as a matter of course. As everyone said, the present is the "era of legalization of security". In other words, administrative security controls and technical security measures operated by companies are being applied by law. Based on this, the unique tasks of the information security department (e.g., policy and procedure establishment, security review, security inspection, security training, security policy violator management, technical security measures, etc.) are executed within the enterprise. Therefore, members who are dissatisfied with corporate administrative security controls and technical security measures should not resist the information security department but against the National Assembly, which is in charge of legal reform. Because, in the current situation where security is legalized, companies. This is because there are quite a few cases where it is possible only to revise the law to reduce security level.

3. Measures to Raise Awareness of Information Protection; Understanding the basic concepts and steps

(1) The basic concept of raising awareness of information security; Thought switch stimulation

In other words, “raising the level of information security awareness” targeting corporate members, It means that we change the thinking of members of Korea in a positive direction. This means that in the end it changes people's thoughts, but it should be seen that it is almost impossible for a third party to change people's thoughts. This is because the area of human thought is a very subjective, personal, and experiential area. Nevertheless, in order to maintain and improve a company's information security system, it is necessary to change the thinking of the members of the company, that is, people in a positive direction. In particular, considering the fact that the contact surface of recent security threats is concentrated as a human factor, and attacks and damage are actually occurring through such contact surface, there is sufficient reason to change people's thinking about information protection in a positive direction.

If so, how can we change the minds of members in order to achieve the goal of raising awareness of information protection, with the premise of changing the minds of corporate members on information protection? To this question, in my experience, it is possible to give an answer that it is possible to “stimulate the switch that people think of”. In other words, rather than directly changing the subjective and personal thoughts of the members, it is to make the members think about information protection through specific issues they have experienced or may experience, and make the choices that the company pursues at the same time for the members themselves according to these concerns. . If you start to raise awareness of information protection based on this concept, the perspective of the members will change from the existing “natural convenience” to “convenient convenience”.

(2) Steps to raise awareness of information protection

The steps to raise the level of information security awareness by stimulating the switch of human thoughts are basically divided into the steps of: i) contact identification ii) step-by-step measures iii) maintenance/improvement. In other words, after finding the point of contact between the level of the information security system pursued by the company and the business convenience that the members of the company thinks of, the step of raising the awareness of information protection step by step and maintaining/improving this point of contact as a baseline.

Figure 4-12 Basic steps to raise awareness of information protection



1) Identification of the interface between perception and reality; Misidentification and Good Identification

① Incorrect identification

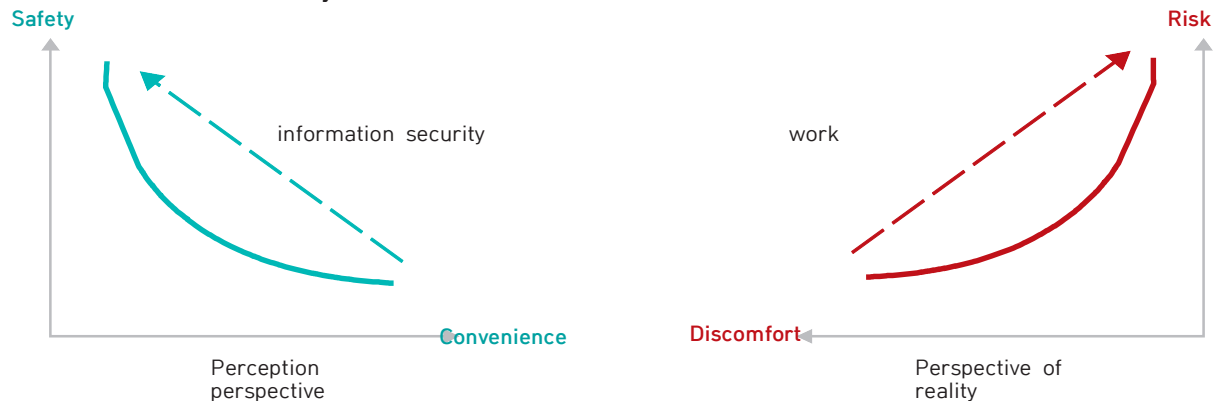
In general, when determining the level of information security awareness of corporate members, it is often judged based on their perception of the importance of information protection. If judged in this way, the level of recognition of the importance of information protection by general employees in the 「2017 Information Security Survey」 should be considered as 81.5%. And from the viewpoint of information protection, the attributes of "safety" and "convenience" are in inverse proportion, and controls using an information security system are applied within the company. That is why On the line connecting these two attributes, the level of security awareness of members is judged (see Figure 4-13).

However, this perspective is only a result of how members think about the direction the information security system pursues. therefore In this result, the general method, that is, business inertia is not included.

On the other hand, when looking at the ways in which the members of the company perform their work realistically, it is understood that they prefer the "dangerous but convenient method" rather than the safe but uncomfortable method". It can be said that the accumulated experience in this way of working has resulted in an inertia to pursue "convenience" in the business process. In a group of members who do not have specific knowledge and experience about "risk" from the viewpoint of information protection, the inertia of pursuing "convenience" in the business process may be a natural phenomenon. Therefore, from the perspective of members who do not directly perform information security work, the attribute of "risk" is not considered, and only the attribute of "convenience" is used

to determine the thoughts and actions of the business process. It is acting as an important determinant (see Figure 4-13).

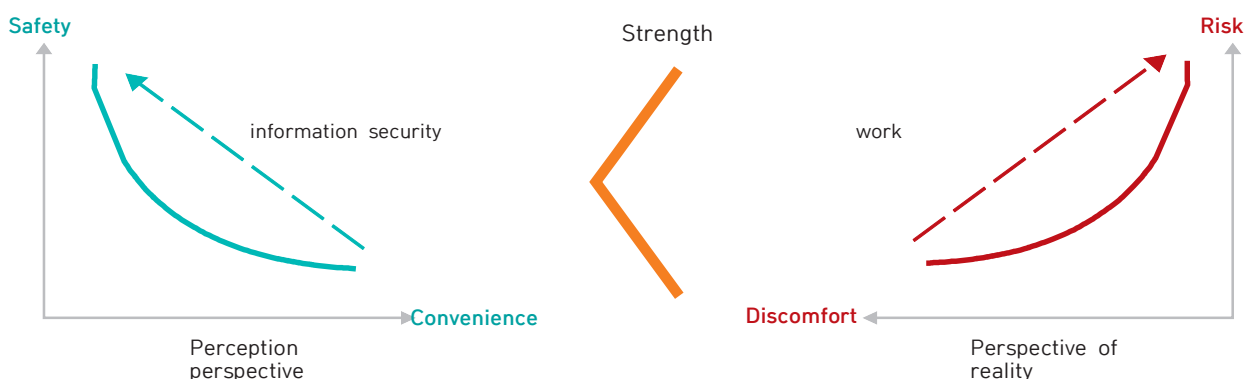
Figure 4-13 (Left) Direction of recognition of the importance of information security system, (Right) Direction of reality based on business inertia



However, from the perspective of the information security department or the Chief Information Security Officer (CISO), which must raise the level of information security awareness, the “inertia of business processing pursuing convenience”, which corporate members take for granted, should not be left as it is. This is because in an environment where employees perform work, the power of the “realistic view to handle business conveniently” is stronger than the “view of perception pursued by the direction of information security”. The reason why the strength of power has such a structure is that the “power of inertia”, which is convenient business processing, is more prevalent than the “power of control”, which is information protection, in the thinking area of members (Fig.4-14).

If it is impossible to “control” this “power of inertia” in a timely manner, “recognition of the importance of information protection” is no longer a subject of great consideration in the process of business processing, and entropy seeking only “convenient business inertia.”

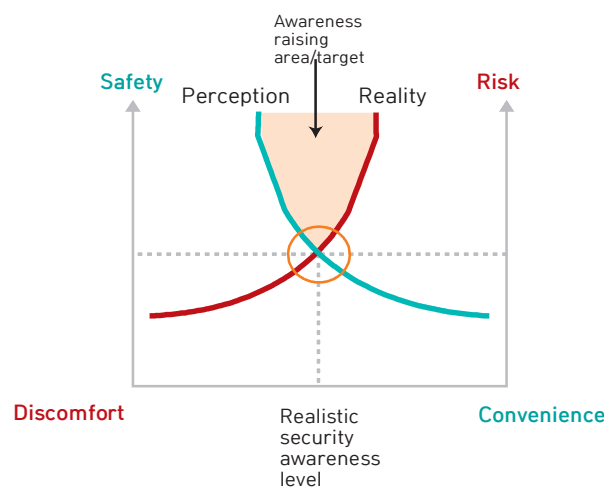
Figure 4-14 Strength of thought between the direction of perception and the direction of reality



② Good identification

Information protection is the most important thing in identifying the contact point between recognition and reality, for raising awareness is to apply the criteria of judgment to the object of judgment. In other words, it is necessary to apply information security controls (standards) targeting corporate members (objects). This is because it is possible to know to what extent employees are accepting the direction that information security pursues through control. Therefore, it is necessary to wisely utilize the inertia of business processing pursuing “convenience” in order to identify the contact point between the perception of information protection and the business reality. In particular, in order to identify a proper contact point, after analyzing the realistic reasons for resistance of members to various controls implemented in the system, the crossing point and gap between these “realistic reasons” and the “controls pursued by the information security system” are identified. It is very important. This is because the crossing point between them becomes a realistic security recognition level, and the gap between them becomes the realm/target of awareness enhancement (see Figure 4-15).

Figure 4-15 Identification of the interface between perception and reality



2) Step-by-step application of information security awareness raising techniques: Continuous upward phase and momentary downward situation

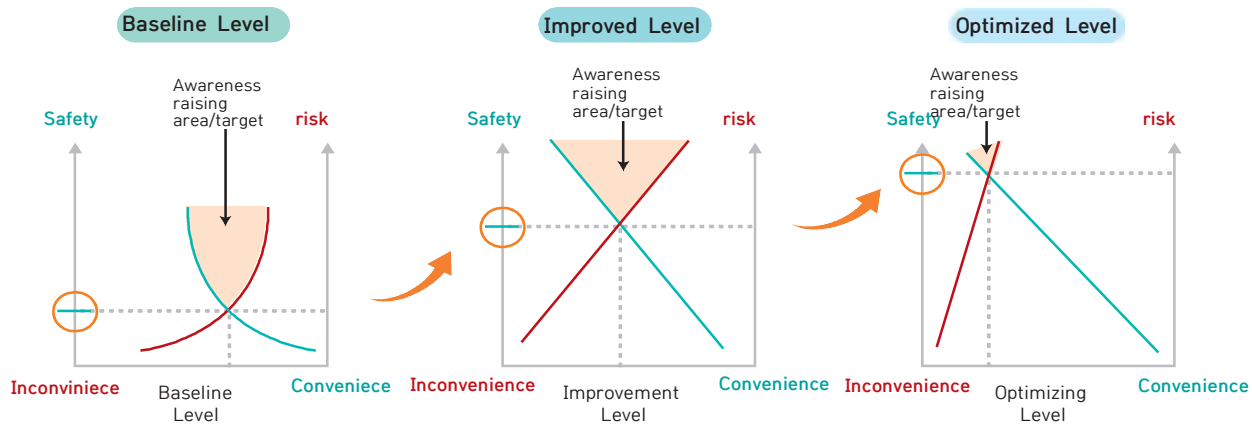
① Continuous ascent phase

After the contact point between recognition and reality, which is a realistic level of security awareness, is identified through the preceding process, The level of this contact point can be set as the “basic level” and various techniques can be continuously applied to improve the level of information security awareness. First, at the “basic level”, it can be said that there is little resistance from members to information security control. This is because not only information security control has little power, but also the “business inertia that pursues convenience” in the work environment of the

members is more dominant (Fig. See 'Basic Level' in 4-16).

When entering the "improved level" stage, members' resistance to information security control begins/increases. This is because the meaning of entering this stage means that the level of the information security system is improving as information security control, which has been hardly exerted.

Figure 4-16 The level of information security awareness is raised



In the past, is exerting its power. In other words, because the reinforced information security system causes discomfort to the members, resistance to it begins, and this resistance goes to a stage where it becomes more and more weighted as time goes by. Therefore, from this "improved level" stage, various controls to raise awareness of information protection. The activity should be carried out (see "Improved Level" in Figure 4-16).

When it reaches the "optimized level", the controls in information security system will exert considerable power. So, at this stage, it is changed into an environment where it is taken for granted that the information security system is observed during the business process. Therefore, activities to raise awareness of information protection for members may be partially reduced. (see "Optimized Level" in Figure 4-16).

To sum up, properly identify the "basic level" stage, which is the contact point between perception and reality, it is necessary to improve the level of information security awareness raising in the 'improved level' stage, and then finally proceed to the "optimized level" stage. As a result of this series of steps, not only the level of information security system within the company will be strengthened, but also the level of information protection awareness in the area of thinking of members will continue to improve.

② Momentary downward situation

It is no exaggeration to say that the most important factor among several important factors is the employee, or the person. This is because people are based on organization and work. This mechanism intact affects the information security system. In other words, information security control is applied to people, information security policies are observed through people, and the information security system is threatened by people. In particular, as information security awareness is in the area of human thinking.

For example, if a new employee enters a company or department that has been working continuously for a long period of time to increase the awareness of information security, the level of information security awareness held by the existing members is shaken by the new employee or the downward curve is changed. There are very many cases of drawing have. The most important cause of this phenomenon can be said to be the “limit of security control over the thinking area” of people. In other words, even if the level of information security awareness has been improved for a long time through various security control techniques, this is the result of the compulsory means of “control”, not the result of voluntary participation among members. That is why the level of information security awareness, which has gone through a continuous rise over a long period of time, is lowered in an instant. Therefore, it is worth remembering that even if the level of information security awareness has reached the “optimized level”, it will not be possible to remain at this level without special efforts to maintain/improve this level.

3) Maintaining/improving the level of information security awareness raising; Culturalization and quantification

In order to maintain/improve the level of information security awareness raising at the “optimized level”, the information security system must be cultured within the enterprise, and quantified indicators that enable this culture to be preserved must be used. In particular, in order to continuously maintain/improve the level of information protection awareness within a company, it is necessary to establish an environment that is not shaken according to the environment of the members (promotion, change of work, transfer of departments, etc.) or changes of the members themselves (new employment, career entry, etc.). To this end, it is necessary to establish a culture that induces voluntary participation of members and apply a means to visually quantify the voluntary participation of members. This will be described later in 6. Security culture settlement plan; From “continuously manageable quantification techniques”, it will be described in detail.

4. Measures to Raise Awareness of Information Protection; Step by step and specific measures

As mentioned above, raising the awareness of information protection of employees is a very important information protection activity that companies must perform at a time when threats that can only be responded to by raising the level of information protection awareness are increasing. However, it is not easy to raise the level of "recognition of information protection", which is the domain of human thinking. If so, how can we increase the level of awareness of information security? The answer to this question will now be elaborated in detail. Of course, in this paper, although the proposed methods cannot be said to be perfect and complete, it would be nice to see them as a solution based on my experience and know-how, who have been involved for a long time in the field of information security, especially in the field of raising awareness of information security.

(1) Contact identification; Understanding of organizational culture

1) Identify organizational orientation

The first step in raising awareness of information security is to identify the "contact between perception and reality". To do this, it is important to first grasp the organization's disposition. The organization referred to here should be 'the whole company', but for convenience of understanding, let's make it a "departmental unit". This is because different departments have different ways and cultures to handle tasks. On the other hand, in the step of identifying the organizational orientation to identify the point of contact between perception and reality, first focus on understanding the orientation, and leaving security measures for each orientation as a future task. It should be applied step by step.

And as a way to understand the organization's tendency, we use indicators of i) whether it is speed-centric ii) how much direction is considered compared to speed iii) whether there is a correction process for the wrong direction. There are two reasons to understand organizational tendencies based on such indicators. The first reason is corporate. Since it is impossible to evaluate the propensity of various organizations in one type, the purpose of substituting three indicators that must be considered from an information security perspective is to subdivide the propensity of the organization. The second reason is that it is possible to know whether there is a security review process in the organization and whether the security review process actually complies.

① Speed Vs. Speed and direction

Awareness and awareness of information protection that the members of the target organization who need to identify the interface between perception and reality and the best way to know the reality that members of this organization are actually doing their job is to first look at whether the organization is "speed-centric". Because, from the point of view of the information security department, we want all

departments organized within the enterprise to consider the safety index "direction (e.g., corporate regulations, especially information security policy, etc.)" as well as the performance index "speed". Most of the organizational reality is considering only the performance indicator speed'.

follow-up security measures Once these organizational tendencies have been identified, CISOs will need to apply administrative procedures and technical means that allow this organization to consider "direction" in the process of performing business in the future.

② Speed and direction; Temporary Vs. constantly

In some organizations, there are organizations that consider direction in addition to the speed of work. Since these organizations have an organizational tendency to consider "speed and direction" together, Compared to that, the level of contact between perception and reality is high.

follow-up security measures If an organization with this tendency is identified, the CISO environment in which the propensity of this organization can be maintained/improved should be constructed. This is because the current organizational orientation may be a temporary phenomenon, and may change at any time when the members of the organization are changed. Therefore, even if the members of the organization change, it is considered a wise solution to construct an environment in which the tendency of this organization can be maintained continuously. As such, for example, the propensity of this organization, which considers "speed and direction" together, is disclosed as a "sample of safe business execution" targeting company-wide organizations. Not only does this increase the likelihood that this organization's orientation will persist, it is difficult for other organizations to ignore sampled precedents.

③ Whether or not there is a correction process for the wrong direction

Suppose there is an organization that recognizes the importance of administrative procedures and technical means related to information security and reflects them in their work. However, in some cases, if the information security procedure is reflected only by the organization's own interpretation, although the information security department must review it, in some cases, the work may proceed in the wrong direction against the information security system. In these cases, determining whether there is a process for correcting the wrong direction can also be an important indicator of an organization's disposition. And organizations with this tendency are more aware of the perception and reality than organizations that consider "speed and direction" together. It can be said that the contact level is high.

follow-up security measures Once you have identified an organization that has these tendencies, the CISO, if you need this organization, utilize remedial processes (e.g. applying security reviews, etc.)

2) Identify the level of compliance

As a way to determine the level of compliance of the organization, the indicators of i) whether you are familiar with relevant laws/notices ii) whether the relevant laws/notifications are applied to work iii) are used to manage changes in laws/notices. The reason for grasping the level of compliance of an organization with these indicators is to determine whether the "security compliance function" is operating within the organization and whether there is a "security review officer" within the organization. In the case of organizations that are managing changes in information protection related laws/notices, most of them have a security review manager.

① Familiarity with related laws/notices

Now that security is legalized, it is no exaggeration to say that information protection, especially customer personal information protection, is a task assigned to all organizations and members of the company, not just the information security department. In addition, because employees are the subject of personal information, they are members of the organization and also customers of other companies. Therefore, you should be familiar with basic laws and regulations and essential notices related to personal information protection. For example, the status of the 「Personal Information Protection Act」 and 「Information Communication Network Act」 in the information security system of companies. These are the main contents that must be observed in the 「Standards for Security Measures (Notification)」. But realistically, the customer's personal information protection business is unique to the information security department and has nothing to do with them. There are quite a few organizations or members who are aware of it.

follow-up security measures Once you have identified these organizations, The CISO should select basic and essential contents that other organizations other than the information security department must comply with based on each statute and notice, notify the company, and periodically monitor it. In particular, if the leakage of personal information is due to an employee's fraudulent behavior, it should be made aware that the employee may be punished under the criminal law (e.g., computer disability, business obstruction, etc.).

② Whether to apply the relevant laws/notices

Recognizing the laws and notices related to corporate information protection and applying them to actual work can be said to be a situation like recognizing the importance of information protection and complying with it realistically. In other words, most organizations are aware of the roles and functions of the 「Personal Information Protection Act」 or 「Information Communication Network Act」, and are also aware of the main contents of the 「Safety Security Measures Standards (Notifications)」 derived from these laws. However, apart from being aware of these laws/notices, few organizations are applying them to their department's business processes. This is because I don't want to do things in an uncomfortable way. However, they are not aware of any laws/notices related to corporate information protection. Organizations that recognize this rather than those that cannot can be said to be higher.

follow-up security measures Once you have identified these organizations, the CISO should select administrative procedures and technical protection measures stipulated in laws/notices related to corporate information protection, and apply administrative and technical measures that can be reflected in the work of each organization. These managerial measures and technical means why you need it and periodic education on how to comply must be conducted in parallel.

③ Whether to manage changes in laws/notices

Laws closely related to corporate information protection (e.g., Personal Information Protection Act, Information Communication Network Act, Credit Information Protection Act) Laws, etc.) are also revised due to revisions to other laws or changes in government policies. In particular, in recent years, revision of the above laws is in progress to find a balance between "protection of personal information and use of personal information". After these laws and ordinances are revised, of course, changes will follow in the contents of the "Standards for Safety Security Measures (Notification)" based on these laws. Therefore, if such laws/notices change, it is necessary to be aware of the contents of the organization performing the related work. If there is an organization that is aware of changes to these laws/notices even though it is not an information security department, the level of contact between the perception and reality inherent in this organization can be said to be high. However, it is highly likely that most organizations that do not perform information security work as their own will not be able to grasp such changes in laws/notices.

follow-up security measures Once these organizations have been identified, the CISO will The latest laws/notifications are selected and notified to the company-wide organization, and the current business process and revised The business process needs to be changed by finding the gap between laws/notices.

3) Understanding the level of understanding of security incident trends

As a method of grasping the level of understanding of the organization's security incident trends, the indicators of i) whether it is a security incident in the same industry ii) whether there is a channel for spreading security incident cases iii) whether or not security measures are established/applied can be used. The reason for examining the level of understanding of the organization on the trend of security incidents using these indicators is This is to determine whether there is a risk assessment process and whether or not a risk assessment has been conducted.

① Whether it is a security incident in the same industry

There is a word called Tasanjiseok. In particular, the information security industry highly appreciates the meaning of this word. This is because there have been many security incidents in Korea since the personal information protection law came into force, and there have been security incidents in a wide variety of industries. In view of this, whether or not the industry is aware of the recent security incidents can be a very important index in identifying the contact point between recognition and reality. Fortunately, among the unfortunate things, personal information protection has become a big issue in recent years, so there are departments that are aware of security incidents in the same industry, even if they are not information security departments. However, in the case of a department that is completely unaware of a security incident that has become a hot topic in the industry, the level of contact between perception and reality is to be rated as low.

follow-up security measures Once these organizations have been identified, the CISO needs to inform the entire organization of the facts of recent security incidents in the industry and the current investigation or trial situation. In addition, for other security incidents that are deemed necessary to be recognized by the entire organization even if they are not in the same industry, facts and investigation/trial situations are selected by category (e.g., external intrusion, internal leakage, exposure, loss, carelessness, etc.). And it is necessary to organize precedents, etc. The data organized in this way are similar outside in the event of a security incident, immediately used as a company-wide announcement material.

② Whether there is a distribution channel for security incidents

When a security incident becomes an issue, the content of the incident security incident must be disseminated to the enterprise organization in order to prevent similar incidents. This is because, through this process, it is possible to raise the awareness of the company's organization and conduct its own diagnosis. However, there is no channel or method to spread the case of security incidents. If it is an organization, the level of contact between perception and reality is low.

follow-up security measures Once these organizations have been identified, CISOs will find and utilize channels through which the information security department can spread security incidents to the enterprise organization (e.g., internal notification window, information security notification window,

enterprise email, enterprise messenger, etc.) Should apply. And if conditions permit, information security It is also necessary to review the use of department security personnel who can spread the case of security incidents propagated by the department once more within each organization.

③ Whether to establish/apply security measures

Suppose a fire broke out because the gas valve was not turned off after using the gas stove in the neighborhood. When encountering such news or articles, it is assumed that we check the gas valve at our house once. I think the organization's attitude toward security incidents is the same. In other words, if a security incident occurring in the same industry is an issue, there should be a function to check whether there is a possibility of a similar incident occurring within our company at least once. If such an organization already exists, it can be said that the level of contact between perception and reality is very high. In reality, the information security department rather than the general business organization will be in charge of such verification. However, what is important here is whether or not the measures or countermeasures after confirming the possibility of similar incidents are applied to the general business organization. In other words, when security incidents in the same industry become an issue, it is necessary to determine whether measures or countermeasures established by the information security department are applied to the company's enterprise organization in order to reduce the likelihood of similar incidents occurring. If security incidents in the same industry are becoming an issue, no measures or countermeasures are applied by the organization within the company. If not, the level of contact between perception and reality is low.

follow-up security measures Once these organizations have been identified, the CISO will be able to prevent an emerging security incident. Possible actions or countermeasures should be established and reported to the CEO first. Because the measures or countermeasures in this case are highly likely to be new measures or countermeasures that have not been applied previously, if applied without the approval of the CEO, the resistance of the general business organization may be high. Therefore, in this case, it is a good idea to first report the need for new measures or measures to the CEO and then obtain approval for application. This will minimize resistance to newly applied security measures or countermeasures. And, if necessary, after a public hearing for the purpose of answering the questions of employees with explanations of new security measures or countermeasures. It is also a good idea to apply it to the warrior.

1) Team play

Since companies generally have a department dedicated to information security work, members of other organizations often think that information security work is only a dedicated department. Of course, there are unique tasks that the information security department must perform (e.g. policy establishment, security compliance review, security review, security check, security training, etc.), but all members of the company are responsible for protecting corporate information. This is a task that can only be done together. In other words, the information security work of a company should be a team play performed by the information security department and other organizations. Maintaining the information security system of a company is not the only job of the information security department, but all members of the company because it is a common value that must be observed.

① Identification of security control acceptance rate

For team play between the dedicated information security department and other organizations, the first thing to do is to identify the "security control acceptance rate" of other organizations. In other words, it is necessary not only to apply security controls based on the "speed of control" from the perspective of the information security department, but also to identify the "speed of acceptance of security controls" from the perspective of the organization that must actually comply with the security controls. For example, if the information security department reviews security for a new business plan established by the planning department, not only the "speed of control" from the perspective of the information security department, but also the "speed of control acceptance" from the perspective of the planning department. Together with the security controls You have to adjust the speed. Because, the meaning implied in the word that the information security system is maintained means that security control and acceptance of control are maintained in both directions, just like a conversation.

② The standard of speed is the other party

As discussed above, the information security system is maintained only when the two-way of "security control" and such "acceptance of control" is maintained. So, what if the speed of security control and the speed of control acceptance are different here? For example, from the perspective of the information security department, Consider a situation in which a specific security control, which is present, is intended to be applied to the enterprise in a short time, whereas the financial department cannot accept the newly applied control in a short time due to the characteristics of the financial and accounting system. In this case, it is desirable to apply the control in accordance with the speed of the financial department (more precisely, the speed of acceptance of the control), not the information security department. Therefore, in this case, the head of the information security department and the head of the finance department decide when to fully apply the new security controls, but gradually applying the new security controls within the scope of not unreasonably affecting the financial department's business processing is important to information security. It can be said to be a way to increase the speed of acceptance of security controls while minimizing resistance to security.

③ Speed control based on reasonable grounds

Information security for the team play of maintaining the system, it is ideal to i) identify the acceptance rate of security control and ii) match the speed of control application to the other department, but in certain cases, it cannot be suited to this ideal situation, and the information security department increases the speed of control. Sometimes you need to increase it. For example, if the existing service or business method is already in violation of security compliance, such as the absence of consent procedures for the use or provision of personal information of the user on the web service, or the destruction or separation of unused user accounts for more than one year. Is like that. In this case, new security controls must be applied to the existing service within a short period of time. There is a reasonable basis for speeding up the speed of security control (e.g. violation of laws/notices, measures to implement security certification defects, measures to implement security check points by government agencies, etc.) In this case, the security controls of the information security department must be quickly applied in cooperation with the relevant department.

2) Communication

The information security department needs to communicate continuously with other organizations in the company. Communication refers to business cooperation meetings, security review, security notices, security training, security checks, and town hall meetings. As such, the reason why the information security department must communicate with other organizations is decentralized information protection. This is to ensure that other organizations also fulfill their responsibilities.

① Security concept from the planning stage!

The planning department or the development department focuses on the novelty of business planning, business feasibility, and feasibility. Therefore, when new ideas or internal/external opportunities arise, we naturally try to realize business planning and system development in a short time. However, from an information security point of view, there is an important problem that appears in this process. In other words, the information security department is requested to check information security related issues when the planning department or development department reaches the completion stage of the business planning and system development. However, in order to resolve the information security issues, it is necessary to return to the initial stage of planning and make corrections. These problems do not end only with the information security department, but can also act as a considerable burden on the planning department or development department. In order to prevent such problems in advance and to use the organization's time efficiently, the department in charge of planning a new business or new service should request a security review from the information security department at the time of planning. To this end, it is necessary to establish a communication channel for the company-wide organization to know the purpose and purpose of the security review and the time of request. Communication channels referred to here may include security notices, security training, and

department head-level meetings. In particular, in this communication process, prior to approval of the proposal by a senior officer with decision-making power, whether or not the plan has been reviewed for security and the result must be asked to confirm what it was like.

② In the other person's language!

When a department in charge of business, service, or marketing conducts business cooperation meetings with the information security department, the atmosphere sometimes becomes harsh. The most fundamental reason that this situation occurs is that communication between the working department and the information security department is not established, so it is only from their own position and viewpoint. However, after some time has passed, if you try to cooperate with the working department again, the cooperation meeting may proceed smoothly unlike the last meeting. This situation arises when expressing opinions with each other taking into account the other's position, not each other's position. In light of this situation, the information security department needs to communicate in the language of the other organization. In other words, it is necessary to communicate using the other department's business processing method and key terms, etc., rather than using only difficult security terms derived from the perspective of confidentiality and integrity. In particular, the information security department often needs to maintain close contact with other organizations in order to maintain the information security system within the company. In the process of maintaining these points of contact, When communicating using perspectives and business terms, the information security department controls administrative security.

③ Positive method rather than negative method

Organizations operating based on expertise, there are areas and standards (eg laws, guidelines, qualifications, experience, level, etc.). The information security department is also an organization that operates based on specialized areas and standards. Therefore, for requests that are contrary to this professionalism, the negative expression is basically inevitable, saying, "That is not possible." However, it is very likely that the employee or department that made such a request was unaware that their request was contrary to their expertise, and most often visit the information security department because they want to know how to implement their request. In such a situation, it is not a good communication method to define only the definition of "no way" because the other organization's request to the information security department violates technical security measures. This is because these situations can be an opportunity to bypass technical security measures. Therefore, in this case, the request of the other organization can be executed without violating the technical security measures. A good communication method is to think about "how to do it" together.

④ Emotion management as a control department

The information security department is the so-called "control department". It is necessary to control the work or procedures of many organizations in the enterprise, and for this purpose, security reviews for new plans, business cooperation meetings, security training, and security checks are conducted. However, in this process of control, there are cases in which the other organization expresses

resentment or resentment. In this case, if the information security department fails to manage the emotions, the information security department may lose its authority as a control department. Therefore, in the security control process, the information security department controls based on business expertise, but does not react emotionally to the other's stimulus.

⑤ Be sure to communicate before applying new security controls

It is natural for the information security department to apply new security controls that did not exist before. It can be thought of as a necessary measure to strengthen the security system. However, from the perspective of other organizations, it can be considered that new inconveniences and procedures arise in the work process. As emphasized earlier, "information security is a decentralized responsibility". Therefore, the application of the new security controls is approved by the CEO.

It is necessary to inform my company-wide employees of the purpose, basis, and compliance method of the new security controls. For example, a town hall meeting where any employee interested in the new security controls that will be coming soon, or a meeting with more than a department head, will make it known. In this communication process, there will be communication between them, and in this process, the resistance that may arise when applying new security controls without communication can be reduced in advance. In addition, if the CEO has already approved the application of the new security controls, the information security department (or CISO) knows directly from the information security department (or CISO), rather than knowing the CEO's approval in writing. It also has the effect of maintaining authority.

3) The aesthetics of waiting

Among the many organizations that make up a company, the employees of the information security department understand the importance of the information security system. I know well. However, this perception also exists among employees of general departments, not information security departments. The reason for this can be said that in the "2017 Information Security Survey", the level of recognition of the importance of information protection by general employees is a whopping 81.5%. However, as described above, there are always phenomena in general departments of "disagreement between perception and reality", "technological security bypass", and "resistance to management security". In order to overcome this situation and maintain the corporate information security system, it is necessary to apply several step-by-step measures as follows. This is because a company's information security system can be maintained.

① Guide rather than control.

Since the basic function of the information security department is "security control", the general department's From the standpoint, I always think of "under control". Of course, if necessary, security controls should be executed for the purpose of the control itself, but if it is not a risky situation, use a "guide" rather than control. That leads to the participation of general departments can be effective.

② Explain, explain, and explain.

Typically, new security processes are implanted inside the enterprise. It seems that it takes more than 6 months. During this period, the information security department is in tremendous activity. The activities referred to here are, for example, security notices and training, town hall meetings and cooperative meetings. In order to implant the new security process into the tissue, it is described in various ways. However, the caveat here is that the security process must be continuously explained even after it has been implanted into the tissue. Because at this point, the security process even in a well-grafted tissue, intrinsic changes within the tissue over time. This is because it occurs. Examples of such changes include changes in the composition of people within the organization, changes in person in charge of work, launch of new tasks, and changes in employee tensions over information security. Therefore, CISOs need to be aware of this situation and establish and apply procedures and methods that can continuously explain the security process.

③ Let them know you are waiting.

81.5% of general employees recognize the importance of information protection. However, compared to this perception, we also examined that there is a discrepancy between the realities in which ordinary employees perform tasks. As a way to minimize such inconsistency, a "method to let people know that they are waiting" can be used. In other words, instead of applying security controls immediately, wait until they request security controls to the extent possible, and let them know that you are waiting. For example, when information that a specific business department is preparing a new business plan is communicated to the information security department, the information security department does not immediately ask the department to do a security review, but until the department requests a security review. Let's wait. And in this process, let us know that the information security department is waiting for the security review request from the department that is planning a new business. In this way, not only can the security review be applied from the initial stage of the planning, but also the procedural awareness that the security review must go through the planning stage can be raised. In addition, the fact that the information security department waited in line with the timeline of the department planning the new business itself is expected to be a good precedent for not only reviewing security but also easing resistance to the information security system within the company.

④ Give enough time for acceptance.

As mentioned earlier, to the extent possible, security controls are not immediately applied, wait, or the reason for continuing communication with other organizations before applying security controls is to give them time to accept security controls. Specifically, I believe that this acceptance is not with the organizations that have spent time as we have often observed that the level of acceptance of information security systems by poor organizations is significantly different. Therefore, before applying the security controls stipulated in laws/policies, the CISO needs to give organizations that need to comply with these security controls an opportunity to think and think sufficiently for a certain period of time. In this way, activities such as meetings and discussions are conducted internally within the organization for a certain period of time, and through these activities, security controls are

psychologically accepted. In my experience, if you are not already violating security compliance, a week or so is reasonable.

⑤ Use the nudge effect.

Establish a policy when the information security department applies security controls. And direct methods such as notification, compliance monitoring and inspection, and violation status management are applied. Of course, these methods are control methods that have purpose and effect in themselves. However, if the purpose is to communicate with other organizations, it is beneficial to apply both direct and indirect methods. The best example of an indirect method is the Nudge method. Nudge here generally means "to stab with an elbow", which is better when a gentle method is applied rather than a coercive method. The result is called the "nudge effect".

For example, suppose that a new policy to prepare for ransomware, which is a big threat, is established, announced, and a direct control method to monitor compliance is applied. In this case, in addition to the direct control method, indirect control using the nudge method can be applied. For example, in order to protect the organization and members of our company, the main content of what the ransomware response officer of the information security department performs and how much labor is the main content, the "daily life of the information security department employee" is made into an in-house announcement article. You can use a known method. In this indirect way, if security controls are performed in parallel, not only does the resistance to direct security controls decrease, but also the capacity of other organizations to actually increase the information security system.

(3) Step by step: Focus on the cause, not the phenomenon

Like violating information security policy. In fact, it can be said that it is a "phenomena" that members deviate from the information security system within a company. And this phenomenon appears as a result of some reason. Of course, from an information security point of view, it is natural to strengthen the security control for this "phenomena" itself. However, if this phenomenon occurs repeatedly, the CISO should consider it deeply. From this point of view, below, there are a few that help you focus on the "cause" rather than the "phenomena". I would like to share some examples.

1) Why the wind is important, not the branches

It is the invisible wind that shakes the branches. Substituting this for cases outside the information security system, it means that the violation of information security is only a "phenomena", and there is a separate "cause" for such a phenomenon. For example, suppose that in the daily security check that is conducted every morning, one employee is leaving documents unattended, and another employee does not shut down the computer when leaving work. In such a situation, neglect of documents and non-shutdown of the computer are only one phenomenon, so the phenomenon itself can solve the problem.

In this case, the CISO should apply security controls by identifying the "cause of the phenomenon" that deviates from the information security system. And the reason why this process of focusing on the cause rather than the phenomenon is important is that through this process, it is possible to identify inherent vulnerabilities of the organization and members of the company and apply specialized security controls to compensate for these vulnerabilities. Therefore, going through a process that solves the "cause" rather than the "phenomena" is a very important step-by-step measure that minimizes resistance to information protection and greatly affects the perception of the importance of information protection.

2) Different security measures by cause

Let's use the previous example as it is. If you want to focus only on the "phenomena", an employee neglects documents every morning, and when such a phenomenon occurs repeatedly, the information security department repeatedly issues an information security violation warning to end. However, this employee repeatedly neglects the documents.

What if it was the location of the employee's desk? In other words, This employee's desk is different from other employees. Since it is in the most inconspicuous corner of the document, if the tension on document neglect is the cause of the document neglect, what security measures would you recommend as a CISO?

In this case, rather than issuing an information security violation warning to this employee, it is much more effective to ask the head of the employee's department to cooperate and change the employee's desk position to a more public one, while minimizing resistance to security measures. It can be a

complementary measure. And if you do this, it will affect other organizations as well, allowing you to correct the behavior of other employees using corner desks. Also get side effects of being.

But in some cases "cause" itself is identified as a very serious situation. For example, let us assume that the computer of an employee who has been on vacation for 10 days before and after the weekend has turned off the monitor but not the main body. To further understand this phenomenon by mobilizing technical systems and equipment available in the information security department, this employee accessed the virtual currency site through a work computer before leaving for the vacation and used the "pre-order and reservation purchase" function. What if you were using it? In this case, it is a "phenomena" that the computer of the employee on vacation is not shut down, and it can be said that the "cause" is that he is accessing a virtual currency site and using the reservation function. However, in this case, if the cause of this is not identified, but only an information security violation warning is issued and the actions taken on this violation are finalized, what would be the perception of other employees who know the cause of this case? Probably, "I just need to take it! Even if you get caught, you only need to get a warning letter!"

Access to unauthorized sites itself could significantly threaten the information security system of a company. Considering that this is possible, it is worth remembering that applying only measures to "phenomena" rather than "causes", especially from the CISO point of view, increases the likelihood of a bigger threat later. Therefore, when the cause of such a phenomenon out of the information security system is a serious situation, appropriate security measures should be applied. In the case of the use of the virtual currency site access and reservation function for long-term vacationers mentioned here:

i) Forced termination of business PC ii) Identification of virtual currency sites that can be blocked and blocking access iii) Company-wide notice on prohibition of access to unauthorized sites iv) The history of accessing and accessing the virtual currency website from this employee's computer identification of all employees present v) identified employees and sending an official e-mail for information security violations to the next senior vi) Requesting an explanation for returning vacationers vii) If necessary, security measures such as referral to the HR committee can be considered.

(4) Step by step: Grounds for investment in information security

1) Laws and guidelines

It is also very important to secure an information protection budget in order to maintain and strengthen the information security system of a company. To this end, in the case of the financial industry, according to the 「Electronic Financial Supervision Regulations」, 5% of the total manpower is made up of IT personnel, of which 5% is composed of information security personnel, and 7% of the IT budget is used as the information protection budget. To use Are doing. However, since these "5-5-7 regulations" are mandated rules for the financial industry, CISOs working in other industries excluding the financial industry are regrettable about the "foundation of information security investment" that can be used to persuade management. . For example, if a new security system is to be built to respond to new security threats, the cost required for the construction will be discussed with the finance department. In this case, the CISO insists on the necessity of construction costs in terms of responding to security threats, while the CFO makes judgments in terms of cost effectiveness. In this case, it is often the case that the cost of construction is not approved in the end according to the opinion of the CFO. How can the CISO convince the CFO in this case?

For securing and investing in the information protection budget of non-financial enterprises, Attached Table 1 stipulated in Article 3 of the "Guidelines on Information Protection Measures" according to the 「Information and Communication Network Act」 can be used. This is because, in Table 1, more than 5% of the IT budget is invested in information protection. It is unfortunate that this regulation is not a mandatory regulation, but a recommended regulation, but the fact that there is a regulation that requires non-financial companies to establish a certain ratio of information protection budget like this can be a big help from the CISO's point of view. Therefore, based on this, it is possible to use a method of requesting an information protection budget from the CFO at 5% or more of the annual budget allocated to all IT departments in the enterprise. In this way, the CISO will make every effort to secure an information protection budget based on statutory basis, even if it is a recommended regulation, and from the CFO's point of view, even if it is a recommended regulation, This is because it puts the burden of decision making.

Of course, this can lead to conflict between the CISO and the CFO. Because the company This is because the CISO has the final decision-making power on my data protection business, and the CFO has the final decision-making power on the budget request. However, even so, the reason why this method should be applied is to allow all members of the company to view information security from a "survival perspective" rather than a "cost perspective".

2) Judicial Precedent

As is well known, there are very many cases of personal information leakage in Korea, and this phenomenon continues to appear even after the Personal Information Protection Act and Information Communication Network Act were strengthened. But at this point Fortunately, among the unfortunate things, the court's judgment on the case of personal information leakage that occurred in the past is coming out. The court's judgment, that is, precedents for personal information leakage, is a very important criterion for CISOs to use in making decisions, and it is also a data that can be used to

secure an information protection budget and earn investment. In particular, precedents that can be used in the process of securing an information security budget are as follows.

Regarding the KT personal information leakage case in 2012, the Seoul Central District Court on January 19, 2018^{Part 4 of the Civil Affairs Office} ruled that "if the information protection regulations are followed, there is no responsibility for the company". There are two implications of this ruling. First, if the information protection regulations are followed, it means that the company has no carelessness in management and supervision. Second, if the information protection regulations were not followed, the company would have negligence in management and supervision. Therefore CISOs need to use this second meaning wisely. For example, the data protection regulations may stipulate a percentage of the annual data security budget, or the CFO may cooperate with the budget requested by the CISO.

In the case of personal information leakage on open market sites in 2008, On January 25, 2018, the Supreme Court ruled, "Even if the notice on administrative and technical safeguards has been observed, it can be admitted that the duty of care has not been fulfilled unless the protective measures reasonably expected from the common sense of society have been taken". In particular, this ruling is a precedent that can be used when an information protection budget is needed to respond to a newly identified threat. In other words, when a new threat is identified as a result of risk assessment performed regularly or necessarily, and additional systems or manpower are required to respond to this threat, the CISO will provide the information protection budget for "protective measures that can be reasonably expected from social conventions". That you can ask for.

On April 14, 2018, the 14th administration department of the Seoul Administrative Court on the case of Pompu personal information leakage that occurred in 2015^{If the personal information protection measures were not done because of the savings, it would be a very serious violation}. In other words, the failure to complete administrative and technical protection measures for personal information protection in order to reduce costs is a "very serious violation" among the standards for calculating the penalty for the Korea Communications Commission. This ruling helps the CISO secure a budget for data protection, especially personal information protection, out of the overall budget within the company.

5. Information Security Education Plan; To Remind Employees of Information Security

Information security education for corporate members is a step-by-step measure that must be applied to raise awareness of information security. Of course, information protection education is one of the security measures applied by many companies to date. However, education that simply conveys content should not be conducted according to the annual information security education schedule. In other words, it is necessary to provide education to raise the level of awareness of information security while minimizing resistance from members through information security education. To this end, we want to share several techniques that can be applied to information security education.

(1) Step by step; You have to switch from the instructor's perspective!

1) A time with "meaning" , not "duty"

Corporate information security department will establish an annual information security training schedule for members and conduct information security training according to the schedule. So, if you're an office worker in Korea, you've probably heard at least one information security education. Have you ever asked them whether the information security education you've heard so far has worked? Or does the information security department see the effectiveness of information security education? Perhaps the answers to both questions are more likely to come out as negative answers. The implication of this word is that the information security education up to now has not been effective. If so, why is the information security education not effective, even though the information security department repeatedly conducts information security education every year for so many hours, and members have repeatedly received information security education every year? The reason for this is that I have not been able to provide "information security education that allows lecturers to change the minds of members". In this judgment based on the grounds, in the end, the success or failure of information security education depends on the instructor's insight.

① Interpretation rather than delivery!

As of today, in an information-based smart society, corporate members must protect customer information. In addition to being a "user" who is obligated to do so, it is also a "user" of other company services. In light of this, current information security education should not be an education that corporate members must attend as "mandatory", but education that is "meaning" for corporate members. Therefore, information security education should be conducted in a way that interprets and understands the policy content, rather than in a hurry to convey the content of a company's information security policy. In order to do so, the contents of the information security policy should be written in the educational PPT. Instead of using time to explain itself, education is focused on good results and bad results in case of non-compliance.

② Cause rather than phenomenon!

As previously discussed, security controls should be applied focusing on the cause, not the phenomenon. Such a mechanism can be substituted for information security education as it is. In other words, to educate specific information security policies in the PPT slide using cases of violating this policy as educational material and introducing specific reasons for violating the policy at the time can be a more effective way to comply with the information security policy. For example, in the slide describing the information security policy of "do not neglect documents," the purpose of prohibiting such acts and how to comply are explained, as well as the specific cause of the violation (e.g. desk location, reservation of virtual currency exchange) Functions, etc.). Of course, it is necessary to share what kind of security controls are applied for each of these specific causes and use them to prevent similar behavior in advance.

③ Use cases when visiting branches/branches

Among the duties of the information security department, there are cases where it is necessary to visit a branch or branch other than the head office to process the business. PC is not shut down, password is attached, screen saver is not set, etc.). These cases become very important educational materials for information security education. For example, in the process of conducting information security training for members of branch it's time to educate about password management policies. At this time, if you present the case of "password attachment" that an employee of the information security department witnessed when visiting branch A in the past and publicly request the branch manager of branch A to prevent recurrence, the compliance rate of this branch's information security policy will increase considerably.

2) Work life Security education itself

① Information protection education by the highest level possible

In recent years, the ranks have been eliminated and the leveled system. There are also companies that have been established, but generally there is a rank system in work life. Such a rank system can be operated not only in the business process, but also in the information security education course with a very good function. for new employees, CISOs directly provide information security education, a virtuous cycle effect can be obtained that has a good influence on the recognition of the importance of information security. Considering the opposite case, this virtuous cycle effect can be understood more clearly. In other words, imagine a situation in which an employee-level employee of the information security department conducts information security training in an educational place where team leaders and above are gathered. Employee-level employees in the information security department will be burdened with the training itself, and team leader-level employees who receive training will not focus on training. Considering such a situation, when conducting information security training, it is effective to be executed by the rank.

② Information protection education that emphasizes the safety of employees rather than the purpose of compliance

At the moment when security is legalized, the importance of security-related laws/guidelines cannot be overemphasized. In particular, due to the legalization of security, not only employees of the information security department, but also all members of the company must fulfill your security compliance obligations. Nevertheless, it is not a good information security education to emphasize only security compliance in information security education. Rather, emphasizing how employees can safely meet their compliance obligations can be far more effective data protection training. For example, rather than the legal responsibility to be borne in case of clicking an email attachment containing ransomware malware, information protection training should be provided that informs the method of selecting such emails and reporting channels. From this point of view, members who have been trained in information security not only have a better understanding of the business areas of the information security department, but also the need for security controls implemented by the information security department.

③ Information protection education that penetrates daily life

That we are teaching information security, in general, education will be conducted according to the annual education schedule, and after that, formal information security education is rarely conducted unless there are special issues. However, there are quite a few opportunities to provide information security education in everyday life at work. For example, suppose an employee in a break room or elevator has made inquiries about the information security system to the CISO. In this situation, you will be able to answer your inquiries within the scope of the information security policy. Of course, since the inquiries were answered from the standpoint of the inquiries, the conversation will end here. However, I would recommend taking it one step further. One step is to send an e-mail to an employee who made an inquiry. That is what the employee inquired with the CISO's answer to this and the basis for the answer (e.g. law or policy, etc.) It is to send an e-mail with your gratitude for giving. If you do this, the employee who receives the e-mail is more likely to be an employee who helps the information security department within the department to which he belongs. In addition, the employee also provides detailed explanations of the inquiries based on the contents of the e-mails he received to other employees who wish to make similar inquiries to the information security department. In my experience, I don't think there is any better way to raise the level of awareness of information security among employees.

(2) Step by step: Discovery of recognition conversion device

The successful factor of information security education is whether it caused a change in the thoughts of members of the information security education. The purpose of information security education should be to change the existing negative thoughts toward positive thoughts. To this end, it is

necessary not only to have a good instructor with deep insight into information security and a high-quality lecture plan, but also to discover a "recognition conversion device" that can be used in information security education. The perception switching device here refers to the switch of the members' thoughts based on news articles or historical events.

1) Different perspectives, different outcomes

There was a very old overpass in front of an elementary school, but it was so old that the stairs were torn down, and there was a hole on the overpass bridge where you could see a car passing by. Regarding this overpass, some elementary school parents have filed a complaint with the competent ward office asking the competent ward office to demolish the overpass, which has the inconvenience of going up and down stairs, and install a crosswalk that allows convenient crossing. However, a few days later, other parents filed a complaint with the competent ward office asking for the maintenance of the overpass. These parents thought, "Although the overpass has the inconvenience of going up and down the stairs, it is a safer means than crosswalks for elementary school children." In response to this, I have seen an article that the competent ward office did not install a crosswalk, but rather repaired the existing overpass more cleanly and robustly. The gist of this article is that depending on the point of view, the results will be completely different.

2) Emotional stimulation

Stimulating the sensitivity of historically wrong things also raises the level of information security awareness. A representative example is the 'walking direction'. Originally, Korea was a country that used to travel on the right from the time of Emperor Gojong in 1905, but it was changed to a left traffic during the Japanese occupation. The reason why the Japanese imperialists forcibly changed the direction of walking in Korea at that time was due to their long-standing habits. Because, in Japan, in the past, samurai carried long swords on their left waist, but if they walked on the right, the possibility of colliding with the sword of the samurai passing by the other side was very high. In the samurai world, the meaning of hitting a sword is a challenge, so to prevent unnecessary killings, Japan has been working since the samurai era. To the left I have been doing it.

Aware of these historical contents, our society launched a movement to change the direction of walking by going to the right. If we explain the reason why our society, which has been 'passing on the left' for such a long time, implements 'going on the right', it is to rethink the meaning of left and right traffic. This is because members who have attended information security education learn new facts through information security education about what they did not know. If you did not know new facts, it is a cognitive assumption to think about new facts. If you use such an awareness conversion device, you only thought 'it should be convenient, of course,' before taking the information security education, but after taking the information security education, you should be 'still safe' or at least, provide insight to corporate members about convenient safety.

(3) Step by step; Message

The members of the company one or two times a year, that is, about an hour or two in information security education. From the perspective of corporate members, through this time, they will be informed of the information security policies that they must know and comply with, and from the perspective of the information security department, use this time to the fullest to strengthen the information security system of the company and the level of information protection awareness of the members. You will want to increase it. However, the problem is that the training time is too short for the information security department, and on the contrary, there is too much content to be delivered from the perspective of corporate members. As such, there is a problem that the effectiveness of information security education does not meet expectations. As a method that can be applied to solve this problem, a 'short message that empowers important information security policies' can be used.

(4) Step by step; Presenting facts that are real but not recognized

1) The reason why the effectiveness of information security education was not good

In our country almost all members of the workplace have been continuously receiving information security education. In particular, as the number of personal information leakage cases increases, the importance of information protection education is increasing. In addition, in the requirements and control items of "information protection certification", the results of information protection training for a certain amount of time per year are presented for members. However, despite this important information security education, it is true that the effectiveness of information security education is not as great as expected. In severe cases, members who have been trained in information security may be more resistant to the information security system. Why does this happen?

The main reason is that members who thought that "information protection is not my problem" could not be educated to recognize that information protection is my problem! after taking information security education. Let's imagine. According to the annual information security schedule, members who go to take information security education during busy hours think that they are trained in an information security system that feels like someone else's work. However, in order to become meaningful information security education, after completing the information security education, these members must let them know that maintaining the information security system is for the members themselves. If the actual dangers that exist behind the convenience that members enjoy are presented based on facts, 'Information protection is I think it can be an effective educational method to recognize that it is my problem!

2) The world behind convenience; Dangerous

Based on my experience In view of this, very good educational effects can be obtained by using a method that informs members of dangerous facts that actually exist but are not recognized by members through information security education hours. In particular, the moment they think it's not my problem, the members become more aware of the information security that becomes my problem. Here are some materials that can be used to raise such awareness as follows.

① The dangers behind Wi-Fi

While I was on the subway, I overheard a conversation between a mother and daughter next to me. The content of the conversation is "Mom, the wi-fi antenna is full, so quickly send money!" In other words, they were asked to do mobile banking in the subway section where the Wi-Fi antenna was well established. Of course, in terms of the convenience that Wi-Fi is free in the subway section and banking can be handled by mobile, you may wonder what is wrong with the conversation between this mother and daughter.

However, in the information security training class, members are notified that there are risks behind this convenience. The 'dangerous' here is the danger that free Wi-Fi is very vulnerable to hacking. If this wi-fi is hacked, it could expose all the wireless access signals that send information to it, just like a lot of insects get caught in a spider web. Therefore, during the information security education time, members are informed of these dangers and are free for their own safety. In the wi-fi zone, it should be recognized to refrain from mobile banking.

② The danger behind smartphone Bluetooth

In terms of fast and easy connectivity, the smartphone Bluetooth provides the best convenience. It can be called a function. This Bluetooth function makes the connection of information between smartphone devices natural, and the convenience of enabling wireless connection with headsets, keyboards, mice, speakers, and even gamepads.

However, even the Bluetooth of a smartphone that provides such convenient functions is important to let members know during information security training that this feature should only be used when needed, and that leaving it on for 24 hours is a very risky option. In my case, there is a question that must be asked to members who are taking training during the information security education class. The question is, "Who sleeps with the smartphone off when sleeping?" When this writer asks a question, most of the members' facial expressions are ridiculous. The reason they make a ridiculous expression is, 'Why do you have to turn off your smartphone when you sleep?' It is used for a variety of purposes, such as setting an alarm for waking up on a smartphone, searching the Internet, and listening to music. It will be a look that comes out of their thoughts without even knowing them. However, the moment it tells you that eavesdropping through a smartphone with Bluetooth turned on is really an entry-level hack, and because of the risk of eavesdropping, some companies are not allowed to hold a smartphone during important strategy meetings. At the moment, the expression of absurdity on the members' faces is disappearing in an instant. I know well. At this time, I emphasized, "If you can't turn off your smartphone, at least turn off Bluetooth!" Members who recognize this fact will at least recognize that the Bluetooth security of their smartphone is a natural measure that must be followed for their own safety and privacy.

③ The danger behind the IP camera

There was a time when it became fashionable to install IP cameras in the house. Especially, if you have pets at home, most of them are managing pets by installing IP cameras at home. This is

because these IP cameras have the convenience of being able to see the inside of the house in real time even outside the house. Is it so? When I was teaching information security, "I use an IP camera at home, if you ask, "Raise your hand, if you have one, two or three employees"

However, even this convenient IP camera can be a target of hacking if it does not take security measures (eg, changing the initial ID and password, etc.). Unfortunately, many IP cameras that have not been secured have been hacked, and there have been incidents in which the privacy of victims in the house is invaded. What I emphasize in the information security education class is "basic security measures". That is, I would have bought an IP camera that if the initial ID and password set at the time had only been changed to an ID and password that only the purchaser could know, such absurd damage would not have occurred. This is because this logic is also in line with the maintenance/improvement of corporate information security systems. In other words, in the information security department. Even if you do not have to explain why you have no choice but to manage ID and password for each member's business computer, it is used for business computers as such IP camera hacking incidents to recognize the importance of protecting IDs and passwords.

Smart TV can install and run programs just like a smartphone or a computer, and can access the Internet and SNS. In addition, it selects programs that suit the user's taste, andIt has a built-in camera, so you can make video calls with someone.

However, Smart TVs equipped with such convenient functions basically use Wi-Fi or the Internet, so they are subject to hacking.The risk of becoming is quite high. In particular, it can be said that the risk of eavesdropping or exposing privacy through a camera or microphone built into the front of the device is higher. I have made these facts aware to the members during the information security training, after which you can use Smart TV "safely". There must be a member who asks questions about how to be.When you receive this question, of course, it will tell you how to use Smart TV safely, but what should be noted here is that there is a desire to know how to use the Smart TV that was purchased "conveniently" and now "safely". to be. These phenomena may be evidence that the thinking of members who are listening to information security education is changing, and that at least information security education is stimulating a switch of thought.

⑤ The danger behind SNS

In recent years, it is not an exaggeration to say that the formation of relationships through SNS is very popular, and there are few people who do not use SNS. Here, SNS refers to public SNS that anyone can see if they have an account (e.g., Twitter or Facebook, etc.) and closed SNS that only those who have signed up can view as well as the account such as KakaoTalk, band, etc.). Such SNS can form a relationship about common interests with people anywhere in the world, and the speed of transmitting information through the relationship is very fast. Therefore, these functions of SNS provide tremendous convenience to users seeking communication.

However, no matter how convenient SNS is, I still do not use it. Because, as I judged by the author who majored in information protection, digital forensics, and law, the SNS space because it has an optimal ecosystem that can be used. The basis for this is that i) the majority of the world is using it (= there are many targets of attack) ii) that the address can be changed (= the attacker hide their tracesⅢ) It is easy to induce clicks (= it is possible to attract victims) iv) Frightening speed (= the

blinking speed of going to the other side of the earth) v) Weakness in social engineering (= authenticity There is no way to check whether or not). Is it so? Recently, there have also been victims of Romance Scams who have been favored by the opposite sex on social media, and then profited from the opposite sex for marriage or business reasons. When I teach information protection, I must make sure that members are aware of these contents, and at the same time do not allow corporate marketing or promotion on SNS, and in particular, emphasize that customer information or business information should not be posted on SNS. have. Because the power of information dissemination on SNS is so great, there are always members who want to do marketing or sales through these SNS channels. Based on my experience, if I first recognize the dangers of SNS and then explain the prohibition on the use of SNS in the information security policy of a company, the acceptance of this will increase considerably.

6. Security Culture Settlement Plan; Quantification of Security Indicators

To briefly summarize the steps to raise awareness of information security, i) properly identify the contact point between awareness and reality ii) raise the level of awareness. The possible steps should be applied step by step. However, as explained above, information security awareness is in the domain of human thinking, so it cannot be enforced or automated. In addition, the level of awareness of information protection is determined by various factors that change within the organization (e.g. change of members, change of work, promotion, turnover, etc.) You can draw a downward curve at any time.

Therefore, the final step in raising awareness of information security should be iii) the step in which security is established as a culture. Because 'awareness' is an individual's domain, it can change at any time, but "culture" is an organizational domain. Because the individual fits into the organization. In addition, if this security culture can be continuously managed and maintained/improved in a quantified manner, raising awareness of information protection will not remain in the domain of personal thoughts that can be shaken at any time, and will be included in the management area of the organization that can be quantified. I will be able to.

(1) Maintenance/improvement: Take advantage of opportunities

Utilizing "internal and external opportunities" as a way to maintain/improve the level of information security awareness raising. For example, the need to obtain security certification, the spread of external security incidents, and the need to participate in government-led training or inspection, etc. Improving It can be a great opportunity to take advantage of. Hereinafter, this will be described in detail.

1) Certification (ISMS-P / ISO27001, etc.)

Security certification is required for companies that are obligated to acquire or maintain security certification under the Information and Communication Network Act. The time to prepare for the audit for the certification and the time to take follow-up measures after the certification audit is completed can be a good opportunity to raise the level of information protection awareness among members. In particular, in the case of companies that are obligated to acquire security certification, 'obtaining security certification itself' becomes an important concern of management, so there is no situation in which working organizations can resist the information security system at all. Therefore, security authentication like this Ready to acquire And the timing of follow-up measures is the best opportunity to secure a "bridgehead for building a security culture."

In addition, it is necessary to meet the requirements of a number of control items in order to obtain security certification.

This is a great opportunity to increase your level of awareness. This is because even members who usually do not have much interest in the information security system must participate or support in

meeting the requirements of the control items during the security certification preparation and follow-up period. And during this process, not only the contact point between perception and reality is naturally identified, but also the level of this point of contact is significantly increased.

In addition, the use of "recommendations and defects" in the security certification audit also strengthens the information security system. Can help. For example, if the members' resistance to the security control that they normally wanted to apply was so high that they could not apply it, if they receive a "recommendation or defect" for the security authentication control items related to this security control, the security control should be implemented within the follow-up period. Applicable measures will be obligatory. This process eventually not only allows you to overcome resistance to certain security controls, but also protects your information. Improve the level of awareness It will be a great opportunity to do it.

2) Security incident case and dissemination of countermeasures

There are many cases of security incidents around us. For example, the media about security incidents include articles, expert commentary, and investigation results and precedents. Among these cases, cases that need to be shared with members should be selected and disseminated to help maintain the level of information security awareness. However, in the case of disseminating cases of such security incidents, it is necessary to maintain the information security system of the company. It is also necessary to select and disseminate cases conducive to the safety of members themselves. This is because it can serve as an opportunity to raise the level of information security awareness by inducing members' interest in security incident cases.

For example, when spreading ransomware security incident cases and countermeasures to company members, it is to spread not only countermeasures to protect work computers and systems, but also ways to protect personal computers and smartphones that members use at home. In this way, when disseminating security incident cases, if the method of disseminating not only the countermeasures necessary for the safety of the individual members as well as the countermeasures from the corporate point of view is continuously used. Information protection is to make them aware of the fact that they are also connected to safety.

On the other hand, in case of disseminating security incident cases to company-wide members, it must be concisely organized and preached. This is because if the content is too long or complicated, members tend not to read the content that has been propagated. Therefore, the content of the broadcast itself is concisely written, and at the end, the entire content is covered with a concise message that you can (e.g., someone who is at ease is not safe!)

3) Government-led training/inspection

Every year, government agencies conduct mock training and security checks to prepare for cyber attacks and to strengthen the information security system. Private companies can also participate in

such simulation training or inspection, and CISOs need to take advantage of the opportunity to participate in such training/inspection. In particular, since such training is conducted in a manner similar to an actual cyber attack, it can be a very good opportunity to recognize the danger of cyber attack and the necessity of an information security system. The same goes for security checks by intelligence agencies. If the CISO applies for such a security check and is subject to the check, it is necessary to carry out activities to improve and strengthen the information security system in preparation for the security check for a certain period of time. This process protects members' information level of awareness naturally raises.

(2) Maintenance/improvement: Share, share, share

This level of information security awareness varies from person to person, task to task, and time to time. It has already been explained that it is possible. In order to compensate for these points, the information security system, the purpose and method of security control, and the expected effects should be continuously shared with members. In my opinion, sharing related to information security work includes a business sharing method (Out-bound) and a personal sharing method (In-bound) as follows.

1) Business sharing: Out-bound

Business sharing refers to a method of sharing with all members. In other words, the information security department becomes a speaker, and company-wide members become listeners. Establishing a new security policy can be said that this is the case when sharing enforcement or sharing security incidents. In this case, the sharing channels are not unified, but various channels (e.g. groupware, email, messenger, security training, etc.)

You need to share through for information security sharing. It is to expose as much of the shared information as possible because there is not much interest. In addition, it is better to share information that is related to the work of all members of the company or that members are interested in sharing through a public hearing. This is because the resistance that will appear in the future can be reduced in advance through this process.

When there are many things to do, it is advantageous to share the security control with high resistance first. This is because security controls with little resistance compared to the previous security controls are relatively easy to accept. And in this event, if several members are resisting the newly implemented security controls, it is wise to persuade the members with the greatest resistance first. Based on my experience, if you openly persuade the member who resists the most, it may later become your greatest helper.

On the other hand, in the case of business sharing in the information security department, it is generally shared at the stage before applying the new security control, and after that, business sharing is not well done. However, since business sharing is considered a service provided by the information

security department, it is necessary to share not only the “previous stage” of applying the new security control, but also the “process” applied and the “time when the application is completed.” This is because through this process, members can recognize that they are participating in the information security system.

2) Personal sharing: In-bound

Unlike business sharing for company-wide members, personal sharing means sharing individual security issues related to a specific organization or specific member. Generally speaking, this is the case when a specific organization or member comes to the information security department for security issues. In addition, it is highly likely that organizations or members who inquire about security issues have already recognized the unique work of the information security department and understand the necessity of an information protection system. Therefore, it is necessary not only to explain the “control standards” recorded in the security policy for security issues that these organizations or members inquire about, but to find a 'safe way to solve it' without violating the security policy. And even after finding a safe way, you should contact the organization or its members to see if there are any additional issues because, even if it is a safe method, if it is a solution that did not exist, a new security issue because it may occur.

(3) Maintenance/improvement: Establishment of objective indicators and utilization

American business scholar Peter Ferdinand Drucker said “if you can manage it, you can improve it.” In the light of this perspective, there are many ways to continuously maintain/improve the level of information security awareness, but if the level of information security awareness can be quantitatively indexed, it will be a more effective method than other methods. Therefore, in the following, information protection indexing the level of awareness. I would like to explain what you can do.

1) Standards for establishing security indicators

Information security awareness exists in the sphere of human thinking. In fact, it is not easy to index this. However, if detailed data and technical means are used, the level of information security awareness in the human thinking area is made into a quantitative indicator. Because people act as they think, thoughts based on objectively revealed actions or outcomes of actions.

① Collection of realistic security indicators

To do this, first, realistically collectible security indicators must be collected for a certain period of time. The security indicators referred to here are the 'security awareness indicators' corresponding to the thinking area and the 'security compliance indicators' that are the result of acting as expected. Examples of security awareness indicators are whether security training has been completed, the number of security reports, personally shared content, and the number of security guide requests. And

examples of security compliance indicators are the number of security policy compliance and the number of security policy violations. Since the more these security indicators are, the more objective quantification is possible, so it is very important to collect many indicators by dividing them into the categories of 'security awareness' and 'security compliance'. In my experience, it is necessary to collect security indicators for at least one year in order to maintain the diversity and objectivity of the indicators.

② How to quantify security indicators

The reason for collecting security indicators is to quantify or quantify them. Realistically collectable as many the method of quantifying security indicators is 'basically a method of giving 100 points'. That is, a specific point in time (e.g. It is a method of assigning 100 points based on the city, etc.), and reflecting the deduction factors and additional points of each security indicator up to a specific end point (eg, at the end of the year or when leaving the company). In this way, you can score 'security awareness' as an area of thought and 'security compliance' as an area of action.

③ Target of security indicator collection

When collecting security indicators, all organizations of the company should be included in the collection. In other words, not only the perceptions and behaviors of individual members, but also the perceptions and behaviors of the organization must be indexed from a security perspective. Therefore, in addition to indexing individual members 'security awareness' and 'security compliance', it is applied to all members of each organization according to the hierarchical organization of the organization to which this member belongs (e.g. office, headquarters, team, part, etc.).

2) Periodic cumulative management

① Application of security indicators

The target for collecting security indicators is determined after the security indicators for each collection target are collected, the security indicators must be applied from a certain point in time. In other words, based on a specific point in time, 100 points are basically assigned to all targets (eg, individual members and organizations), and then the factors of deduction and additional points of each security indicator are reflected. In order to effectively apply the security indicators to all members and organizations, it is best to apply it in an automated manner, such as establishing a system on its own, but if there is no room, it is basically 100 points on the Excel sheet for each security indicator collection target. Is given, and points are deducted on the 'security awareness' and compliance' indicators and it can be applied in a manner that reflects it as a numerical value when an additional point factor occurs.

② Share the status of security indicators

If you start applying security indicators from a certain point in time, the status of each department's

security indicators should be periodically shared. For example, on a quarterly or semiannual basis, the score of each member of the department and the score of the security index of the entire department are shared with the head of the department. In this way, the head of the department will be able to make an intermediate check on the level of security awareness of the department he manages, and for the remainder of the period, administrative efforts will be made to increase the level of security awareness within the department.

3) Company-wide disclosure of security indicators

① Ranking by department/individual

For example, since the final result quantified from a specific point in time to a specific end point, such as from the beginning of the year to the end of the year, is derived as a score, it is possible to rank each department and individual members based on this score. In other words, the score of Department A is 99 points, and this score is the first in the company-wide department score ranking, and the score of Hong Gil-dong is 95 points, and this score is 4th in Department A and 26th in the entire company.

② Annual security indicators and rankings are reported by the CEO

Security indicators and rankings aggregated over a certain period of time must be reported to the CEO. Because the CEO is also included in the security index collection target, the CEO's own awareness is raised. In addition, the importance of the ranking of security indicators can be recognized by all members.

③ Apply compensation and complementary measures corresponding to the ranking

When the rankings of the security indicators are aggregated, compensation corresponding to the upper ranking and a method to supplement the lower ranking must be applied. From my experience, I think the best compensation and supplementation plan is to connect with personal KPI and personnel system. For example, if the security index is more than 90 points, the department head should give the member additional points to the individual KPI, and if the security index is less than 70 points, the method is excluded from the next year's promotion. Since this enables personnel management based on quantified figures, it is considered to be a highly preferred compensation and supplementation plan not only for department heads who evaluate KPIs, but also for personnel departments.

④ Review the rationality of security indicator standards every year

It is not possible to apply the same standards every year without adjusting the security indicator standards once established. This is because the organization's work, members, and security policies change according to the flow. Therefore, the standards of security indicators should be reviewed annually for rationality. And, as a result of such a rationality review, the standards of the revised security indicators should be shared with all members to minimize resistance to the security indicators.

And through such a process, more objective standards of security indicators will be established, and security indicators applied based on these standards are essential for the formation of a security culture.

7. Epilogue

(1) Limits of information security awareness

In order to raise the level of information security awareness, we have identified awareness and reality, applied various step-by-step measures based on this, and finally looked at the stage of making security a culture. As Peter Ferdinand Drucker said, "Culture eats strategy", it is more effective to make security a culture rather than step-by-step measures to raise information security awareness.

However, there is an unavoidable limitation in "information protection awareness", which will be described in detail below.

1) The phenomenon of difference occurs: People, environment, time

The level of awareness of information security varies depending on a number of factors. For example, even in the same department, the level of awareness of information protection is different for each member, and the level of awareness of information protection is different every time depending on the environment in which work is performed and the time. In this "phenomena of difference", the perception of information protection. It appears to be a phenomenon that appears because it corresponds to the area of thought.

2) Impossible to automate: Human thinking sphere

The second limitation of the perception of information security in the realm of human thinking is that "automation is impossible". For business computers and servers, the security environment can be set automatically by applying a policy in the security system, whereas human thoughts cannot but be automated or enforced. Therefore, raising awareness of information protection is an important and difficult to realize from an information security perspective.

3) Environmental impact: an easy return to convenience

No other area will be affected by the environment as much as information security awareness. In particular, the fact that the force of inertia to return to the convenience is very large. This is the third limitation. For example, suppose that the level of information security awareness of a department has increased considerably as a result of the information security department's continuous and step-by-step efforts.

Now the department naturally embraces security processes in the business process and to reflect after a new experienced employee joins this department, what if he complains that the security level of this department is uncomfortably high compared to the security level of the company he attended? This complaint can be a complaint that instantly undermines the level of information security awareness.

4) Vulnerable to "user traction '

From an information security perspective, users are employees of the company and users are customers. Therefore, when employees stand in the position of users, they comply with the company's information security system and increase the level of information protection awareness. However, when a user, that is, a customer, complains about the information security system, the direction of the employee's perception of information protection draws a downward curve again. For example, if an employee who is using a password by making a password complex according to a secure password policy hears from a customer that it is uncomfortable to make the password for the customer too complex, the employee applies it to his work computer, etc. They think that even the passwords that have existed are unnecessarily complicated. After all, this thought, again, can lead to resistance to administrative security.

(2) Complementary Measures for Limits in Information Protection Perception

As discussed above, we have to admit that there are inevitable limitations inherent in information security awareness. Nevertheless, the CISO who must maintain and improve the information security system must manage the level of information protection awareness by using measures that can overcome or at least supplement these limitations. As a complementary measure, not only a plan to use technical means, but a plan to use administrative procedures and the like, which will be described in detail below.

1) Continuous monitoring and behavior analysis

In general, people behave as they think, but in companies there are several systems that can check the behavior of members. For example, there is a network access control (NAC) system, an information leakage prevention (DLP) system, or a firewall (F/W). Of course, such a system is basically a system that is operated to maintain the information security system of a company, but in such a system, members' actions can be checked.

Indirect indicators (e.g., access logs, PC power failure time, malicious code infection status, etc.) are accumulated every day. Using such indirect indicators, it is necessary to continuously monitor the information protection awareness of members by adding or subtracting the scores of the "security awareness" and "security compliance" indicators. And by monitoring these indirect indicators, the situation of internal security threats may be observed outside the situation of adding or subtracting security indicator scores. In such a case, by using several indirect indicators accumulated in the security system, It must be analyzed and it may be necessary to switch to security audit.

2) Periodic security awareness assessment

Under the premise that people's thoughts can change at any time, members' perceptions of information protection should be periodically evaluated. For example, shared quarterly or semiannually. It can also be evaluated through the status of security indicators by department. Also, as shown, it can be evaluated through indirect indicators accumulated in the security system, and also through the results of security checks or complaints about the information security system. Therefore, the CISO should periodically evaluate the members' perception of information protection through the process of evaluating security indicators, evaluating indirect indicators, checking security, and collecting security complaints.

3) Establish a security philosophy in the decision-making process

Keeping the level of information security awareness at a certain level is not easy, but if "information security issues" must be taken into account, at least a certain level of information protection awareness can be maintained for matters for which decisions are made. For example, when a department head or higher makes a decision, that is, approval within the given authority, the decision-making process is systematized so that the "information security issue" must be reviewed for the subject for approval. In this way, information security issues are reviewed from a practical point of view at the time of approval by the department head, and "information security issues" are checked from a managerial point of view in the decision-making process in which the CEO finally makes an approval through the second-level supervisor.

4) Use of Security Statement

Another administrative measure that can be used to keep all members of the company at a minimum level of information protection is to write a "security declaration", receive the CEO's signature, put it in a frame, and attach it to each office and conference room. For example, along with a simple security statement, a security statement signed by the CEO is affixed at the bottom of the phrase "customer's information belongs to the customer". In this way, it can be used as an important criterion for business disputes with the working department regarding the information security system.

The measure of the maximum limits is the management philosophy on information security.