Preventing the Unwanted Transfer of Technology

警察庁
National Police Agency

National Economic Security Office (With cooperation from the Ministry of Economy, Trade and Industry)

Introduction

Recently, the term *economic security* can be seen daily in newspapers and other news media.
Why is this term used so often now?

- Increased competition among nations
- The emergence of innovative technologies such as AI and quantum technology
- The emergence of new security domains such as space, cyberspace, and the electromagnetic spectrum
- Vulnerabilities in supply chains which have surfaced due to the COVID-19 pandemic and other challenges

These various developments have increased the occasions, in the fields of economy and technology, in which national security must be taken into account.

In light of this situation, many countries are promoting measures to ensure national economic security, such as government assistance to strengthen industries, prevention of the unwanted transfer of important technologies, and strengthening of export controls.

In Japan as well, measures are being promoted with the aim of improving economic autonomy and developing superior and thus indispensable technology while maintaining and strengthening international order.

In Japan, there are many private companies and academic institutions possessing advanced technology, some of which could be used for military purposes. If such technology is transferred to a foreign country, the international competitiveness of Japanese companies will be undermined, and Japan's security may also be seriously affected.

Prevention of technology transfer is now an important economic security issue.

In an effort to address this issue, the police are encouraging private companies and academia to take preventative measures through outreach activities in which the police provide information such as methods previously used by foreign countries to obtain technical information, and possible ways to counteract those methods.

As part of such outreach activities, this booklet aims to provide managers, employees, and researchers of companies and academic institutions with information on how the unwanted transfer of technology occurs and what to do to prevent it.

It is our hope that this booklet will be used by readers to step up their current countermeasures.

August 2022

Table of Contents

To Prevent the Unwanted Transfer of Technology

01 Be aware of the situation

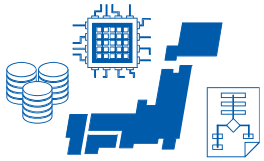
02 Be aware of examples

03 Be aware of countermeasures

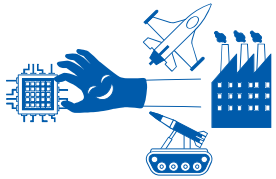
To prevent unwanted technology transfer, it is important to be aware of the situation, examples of technology transfer, and countermeasures.

Situation: What is happening now?

In recent years, geopolitical risks have come to the fore, and international industrial competition has intensified.



In Japan, there are many private companies and academic institutions, large and small, that possess advanced technology.



They have become targets for foreign countries that want to acquire such technology to strengthen their own industries or to divert it to military use.

Prevention of technology transfer has become an economic security issue.

Examples: How does the unwanted transfer of technology occur?

The risks that technology possessed by private companies and academia may be targeted by foreign countries can be broadly categorized into three types.

Types of technology transfer risks

1 Technology transfer via cyberattack

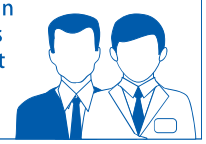
Cyberattacks targeting government organizations and critical infrastructure operators are increasing in intensity both at home and abroad. As digital transformation (DX) progresses in all industries, the risk of information being stolen directly through cyberattacks and unauthorized access increases.

2 Technology transfer via espionage

In addition to risks in cyberspace, caution is necessary with regard to information theft using a person in the real world. For this type of risk, we need to be watchful for cases in which a foreign country recruits a spy to gain access to and then steal a target company's information.

3 Technology transfer via business/academic activities

As business activities become more globalized and research activities become more international and open, we face an increasing risk that legal business and academic activities —such as joint ventures, corporate acquisitions, and joint research—will be used as covers to obtain targeted information.

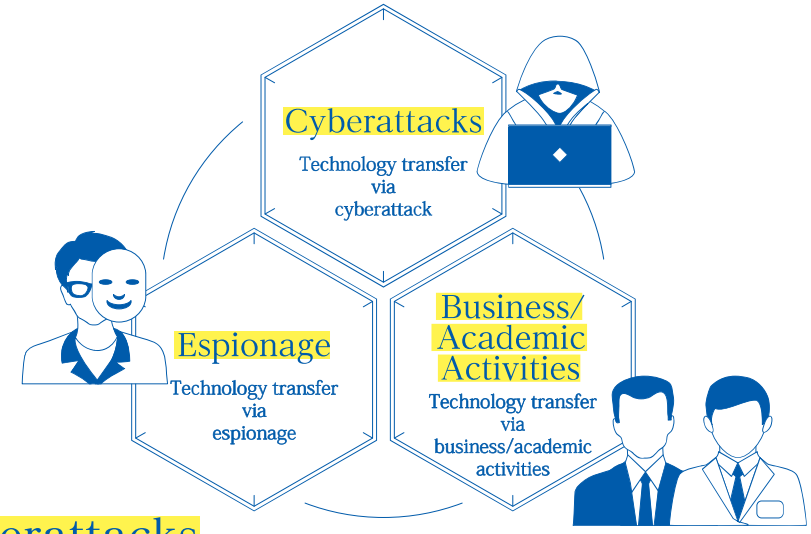


Countermeasures: What should be done?

It is important that each and every one of us is aware of the methods as well as the risks of technology transfer and that basic countermeasures are taken. The following pages provide tips and essentials for this awareness. Please make use of them in your daily activities, being aware that it may happen to you as well.

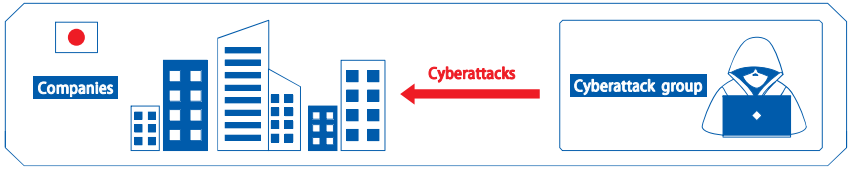
How does the Unwanted Transfer of Technology Occur?

Let's examine some real–life cases investigated by police and also where the risk of unwanted technology transfer was increased.



Cyberattacks

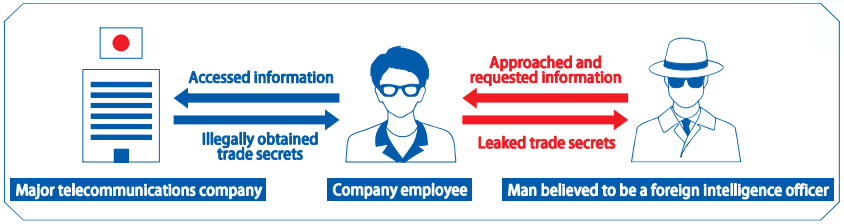
CASE 1 In 2021, the Metropolitan Police Department sent a public prosecutor the case of a man known to be a member of the Communist Party of China suspected of renting Japanese servers by registering with false information, such as a fake name and address, between 2016 and 2017. During the investigation of this case, the police found that cyberattacks targeting an aerospace organization were conducted by a cyberattack group very likely linked to China's People's Liberation Army. The police strongly believe that the same attack group was involved in the targeting of approximately 200 companies and other entities in Japan.



CASE 2 A Japanese company doing business in a foreign country was requested by the foreign authority to provide technical information while negotiating its relocation to a special economic zone. On the day it rejected the request, the company began suffering cyberattacks.

Espionage

CASE 1 The Metropolitan Police Department handled a violation of the Unfair Competition Prevention Act involving an employee of a major telecommunications company and a Russian believed to be an intelligence officer. The employee was suspected of illegally obtaining company trade secrets—information on field trials related to its wireless base stations—between February and March 2019 and passing the information on to the Russian.



CASE 2 Multiple employees of Japanese companies possessing advanced technology were approached on their way home by a foreign government employee on the pretext of asking for directions. The foreign employee then invited each of them for a drink on a later date.

Business/Academic Activities

CASE 1 A university in Japan concluded an exchange program agreement with a foreign university after specifically including an export control clause concerning prevention of information leaks. Later, however, the foreign university requested to redraft the agreement anew. When the Japanese side checked the contents of the draft, it found that the export control clause had been deleted with no explanation.

CASE 2 A foreign company proposed a joint research project to a Japanese university professor. The professor declined because the company was on another country's restriction list. The company then proposed to use the name of another company as a cloak.

First Things to Do

Specifying and Managing Confidential Information

Three Steps

To prevent the unwanted transfer of technology, it is important to understand and implement the following three steps.

STEP 1	STEP 2	STEP 3
Identify and evaluate the information held by the company and then determine which information should be confidential	Classify the confidential information	Determine the measures to be taken according to the classification of the confidential information

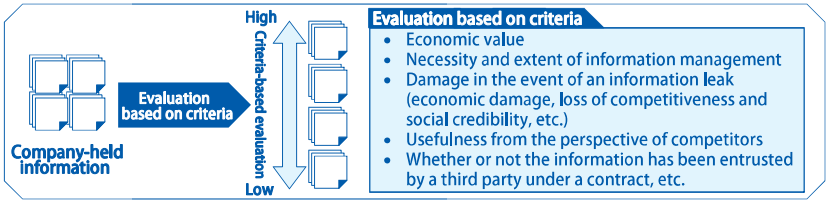
STEP 1 Identify and evaluate the information held by the company and then determine which information should be confidential

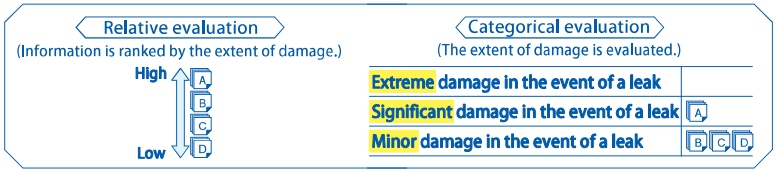
(1) Get an overall picture of the information held by the company

Verify what information the company holds. Information exists not only in the form of paper or electronic data stored in PCs and servers, but in invisible forms as well. For example, manufacturing know-how acquired by employees in the course of work that is not documented is invisible. Caution is advised not to overlook any information.

(2) Evaluate the information held by the company

Evaluate the information in question based on such criteria as economic value and possible extent of damage in the event of an information leak.





(3) Determine which information should be confidential

Determine if a piece of information is worth protecting by how high it ranks for various criteria. Take a comprehensive view of possible administrative costs, litigation costs, potential damage caused by a leak, and other factors.

STEP 2 Classify the confidential information

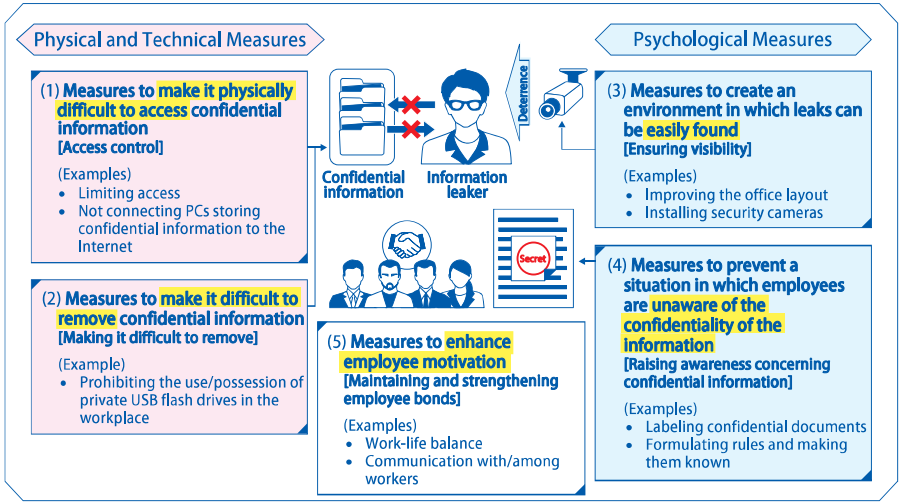
Classify the confidential information according to management level, based on such factors as the content and nature of the information, how high it ranks for various criteria, how it is used, and possible measures for management. It is important to strike a balance between protecting information and maintaining ease of access during daily work.

STEP 3 Determine the measures to be taken according to the classification of the confidential information

For each classification of confidential information, determine specific measures to be taken to prevent information leaks. Effective countermeasures differ depending on the situation, such as against whom the measures are taken, in what form the confidential information exists, and what the method and motive of the leak might be. The determination will also differ depending on whether or not teleworking has been introduced, so choose measures suitable for the company.

Five Categories of Measures to Prevent Information Leaks

Measures to prevent information leaks can be broadly classified into five categories. Companies are advised to be aware of these measures, as well as their aims, and promote them among their employees.



(Source: *Handbook for the Protection of Confidential Information* by the Ministry of Economy, Trade and Industry)

Countermeasures (1)

Cyberattacks

Measures against Cyberattacks

Three Basic Measures

1 Risk reduction measures

- Strengthen authentication by such means as checking for overly simple passwords, checking access authorizations, using multi-factor authentication, and deleting unnecessary accounts.
- Verify the status of information assets as well as IoT devices. In particular, vulnerabilities in devices that control Internet connections, such as VPN devices and gateways, are often exploited in attacks, so security patches (latest firmware, update programs, etc.) should be applied promptly.
- Inform employees that they should not open e-mail attachments carelessly, should not click on URLs carelessly, and should consult with appropriate contacts immediately if there is anything suspicious.

2 Early detection of incidents

- Check various logs on the server and other devices.
- Review how communications are monitored/analyzed and access is controlled.

3 Appropriate response and recovery in the event of an incident

- Go over the data backup and recovery procedures to prepare for data loss and other incidents.
- To prepare for possible incidents, go over the procedures to be followed should one occur, and establish an external response in addition to internal communication systems.

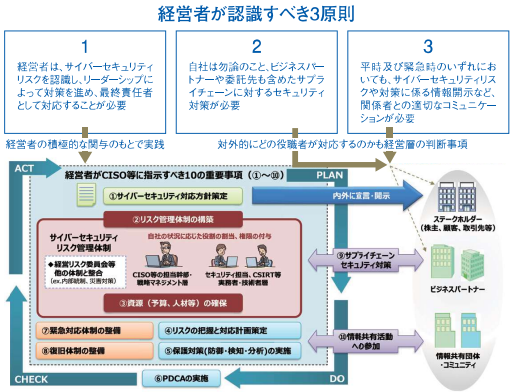
Drawn up by the Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency, Japan (IPA), *Cybersecurity Management Guidelines* presents corporate management the principles needed to be recognized and the directions (e.g., Build a management system for cybersecurity risk.) that should be given to the executives in charge of cybersecurity.

サイバーセキュリティ経営ガイドラインVer 2.0実践のためのプラクティス集 (Cybersecurity Management Guidelines Ver. 2.0 Practical Applications) compiled by the IPA includes the concerns of security personnel and offers specific examples of how problems were dealt with.

Both documents will be helpful in taking cybersecurity measures. Please use them in conjunction with the three basic measures against cyberattacks explained on the previous page.

Principles for Corporate Management and Building a Cybersecurity System

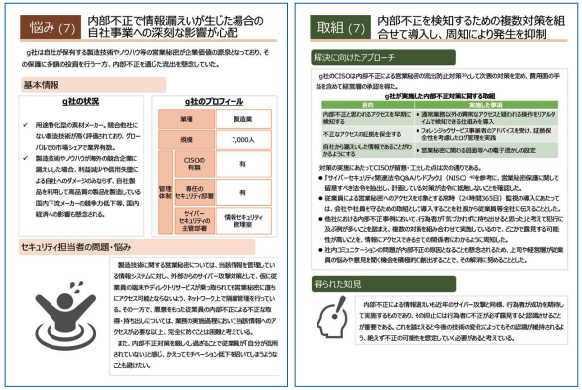
- Cybersecurity principles corporate management should know
- Important cybersecurity measures explained



(Source: *Cybersecurity Management Guidelines Ver. 2.0 Appendix F* by METI and IPA)

Specific Measures

Learn in detail what to do to address cybersecurity concerns.



(Source: *Cybersecurity Management Guidelines Ver. 2.0 Practical Applications* [3rd ed.] by IPA)

Countermeasures (2)

Espionage

Measures against Espionage

Three Ss for Each Individual to Act on

1 **See** Observe people carefully

2 **Stop** Take time to think

3 **Share** Consult and communicate

Have any of these happened to you?

- ☑ A message was sent to your social networking site from a foreign company with which you had no contact.
- ☑ A foreigner you did not know spoke to you on the street.
- ☑ An employee of a foreign company with which you have business relations gave you a gift or treated you to a meal as a token of thanks.
- ☑ An employee of a foreign company asked you to provide information to which access is limited.

These are some of the signs that foreign actors may be targeting you for espionage.
What can you do to protect yourself from espionage?

See Observe people carefully

See the affiliations and contact details of people when meeting outside of usual business settings, such as in your private life or on a social networking site.

- Everyone is at risk of becoming a target for espionage.
- There are cases in which someone seemingly approaches you by accident, having actually researched you already, in an attempt to obtain information from you by such means as invitation to a meal.
- Discrepancies between a person's remarks and profile and whether or not the person's company really exists are possible warning signs.

Stop Take time to think

Stop and think before you post your personal information to a social networking site or any other site where it can be seen by the general public.

- While social networking sites are useful, foreign actors may glean personal information from such sites, using it to approach or threaten their potential targets.

Stop and think before receiving a gift.

- Gifts and meals may put you in a "difficult-to-say-no situation," which may later be exploited to obtain information from you. Think rationally about the motive behind the personal gift.

Share Consult and communicate

Even if it seems trivial, **share** what is happening with your supervisor and colleagues. If there is anything suspicious, please contact the police as well.

- Foreign actors usually take aim at their targets secretly. When you are contacted by a stranger or approached suspiciously, discussing it with someone will help you make a cool judgment. By sharing, you prevent people around you from becoming targets.
- If you are too careless when asked to provide information, thinking "this information is no big deal" or "it's okay because he/she is a nice person," valuable technology may be given away, and, worse still, you might be charged with a crime.

Countermeasures (3)

Business/ Academic Activities

Measures for Business/Academic Activities

Three Ss for Private Companies and Academia to Act on

1 **See** Examine the company and documents carefully

2 **Stop** Take time to assess the risks

3 **Share** Consult and communicate

While collaboration with a foreign company—such as establishment of a joint venture and implementation of a joint research project—provides an opportunity to raise corporate value, it also carries the risk of unanticipated technology transfer.
At a time when it is said that such risk could affect Japan's national security, what can private companies and academia do?

See Examine the company and documents carefully

See the foreign company with which you are dealing.

- What is important is not to hold back from joint ventures, corporate acquisitions, and joint research involving foreign companies, but to recognize the risk of technology transfer that may exist in such activities.
- Having an expert do a background check of the foreign company helps.

See the documents to recognize the risk of technology transfer.

- Carefully check the contents of the agreement and other documents.
- If you trust the foreign party and fail to check, important items such as an export control clause may be deleted without explanation. It helps to have the agreement checked by the section in charge or outside experts.

Stop Take time to assess the risks

Stop and assess the risks in activities that could lead to the inadvertent providing of technology to a foreign country.

- There was a case in which a foreign company pointed out inadequacies in equipment just before an agreement was reached, and the Japanese side was requested to show design drawings and provide the equipment prototype. In a case like this, there is a possibility that sensitive technology could be revealed via the provided equipment.
- In addition to the risks of expanding abroad and establishing a joint venture, risks associated with pulling out of a foreign country and dissolving a joint venture are also points to check.
- It is also effective to exchange information within your industry about the foreign country's laws and regulations and cases involving risks.

Share Consult and communicate

If your business involves providing sensitive technology, share and communicate with your colleagues in relevant sections.

- If your attention is focused on reaching an agreement, you may become careless about export control and trade secret management, ending up violating relevant laws and regulations by mistake.

If you notice a suspicious maneuver, please consult with relevant organizations and the police.

- Transfer of technical information is irreversible.
- When something suspicious occurs, to prevent the unwanted transfer of technology to a foreign country, please consult with relevant organizations and the police.

Foreign educational videos about the prevention of unwanted technology transfer

FBI

The Nevernight Connection

(With Japanese subtitles)

FBI

The Company Man: Protecting America's Secrets

(With Japanese subtitles)

ASIO

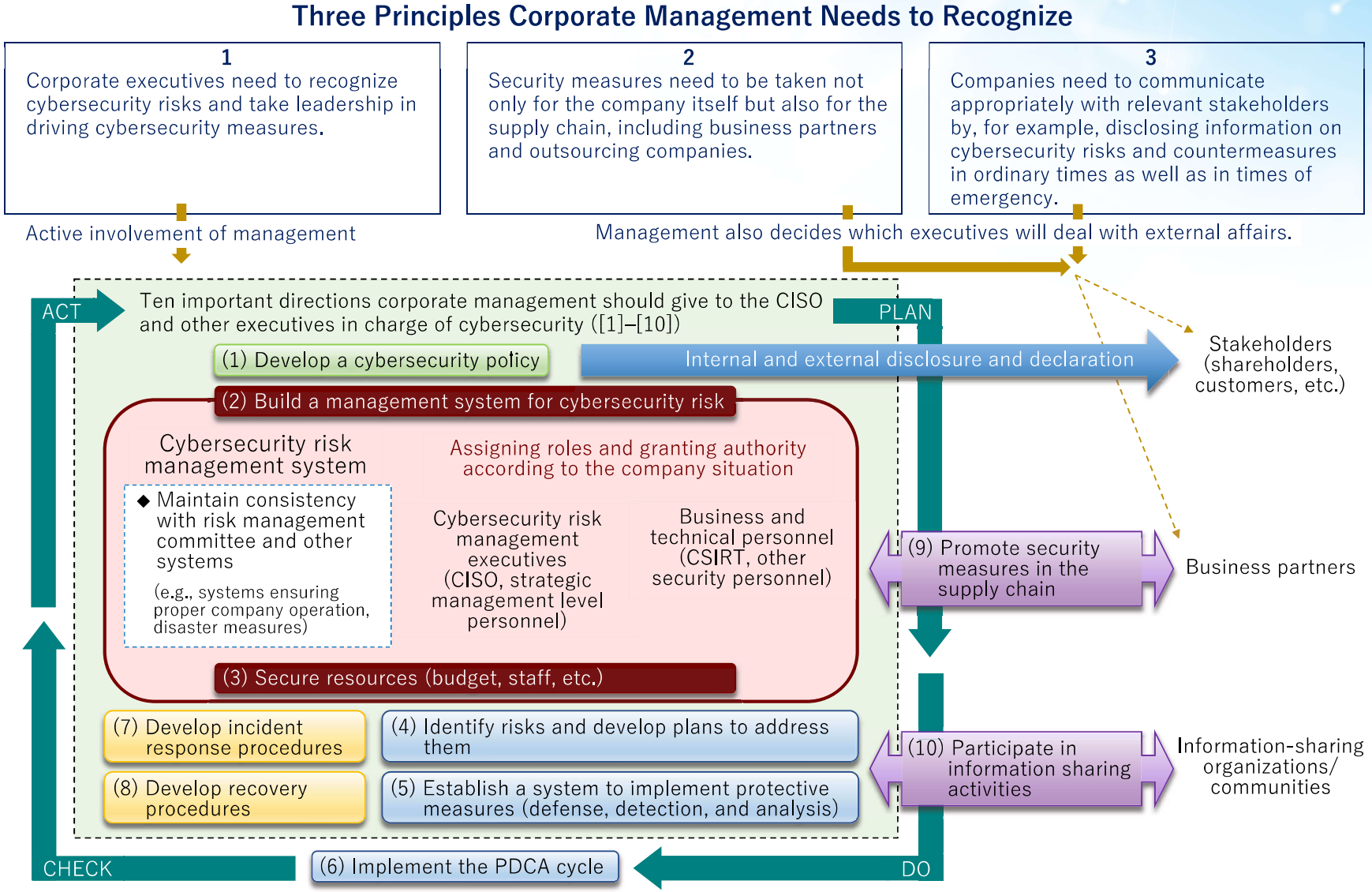
Jack's Story- Think Before You Link

FBI：Federal Bureau of Investigation（米国連邦捜査局）
ASIO：Australian Security Intelligence Organisation（オーストラリア保安情報機構）

National Police Agency
National Economic Security Office, Foreign Affairs Division, Foreign Affairs and Intelligence Department, Security Bureau
keizaianpo110@npa.go.jp

Appendix A

Translation of the Page 10 Diagram Taken from *Cybersecurity Management Guidelines Ver. 2.0 Appendix F*



Appendix B

Translation of the Pages from *Cybersecurity Management Guidelines Ver. 2.0 Practical Applications* Reproduced on Page 10

Concern (7) The company's business may be seriously affected if information is leaked through internal misconduct.

Company G's trade secrets, such as its manufacturing technology and know-how, are a major source of its corporate value. Investing heavily in protecting these secrets, the company is apprehensive about possible leaks resulting from internal misconduct.

Basic Information

Situation of Company G

- ✓ Company G is a manufacturer specializing in producing materials for specific uses. Its manufacturing technology not possessed by competitors is highly valued and largely responsible for its prominent position in the global market.
- ✓ If its manufacturing technology and know-how are leaked to foreign competitors, the company's profit and credibility will suffer. There is also concern that Japan's economy could be affected by a decline in the competitiveness of domestic downstream companies that manufacture high-quality products using company G's products.

Company G Information

Industry		Manufacturing
Company size		7,000 people
Management system	Does the company have a CISO?	Yes.
	Does the company have a dedicated security section?	Yes.
	Section in charge of cybersecurity	Information Security Management Office

Problems Facing Security Personnel

As a measure against cyberattacks from outside the company, the information system that manages trade secrets concerning manufacturing technology is isolated from other networks so that they will not be immediately accessible should the directory server or computers be compromised. However, when it comes to illegal acquisition or removal of trade secrets by an employee with malicious intent, Company G's security personnel find complete prevention difficult, as access to such information is necessary in the course of work.

Also, overly strict measures preventing internal misconduct are undesirable since employees may become less motivated, feeling they are not trusted.

Actions Taken (7) A combination of measures against internal misconduct was introduced and made widely known with the aim of deterrence.

Approach to Problem Solving

The CISO of Company G decided upon the measures shown in the table below to prevent the leaking of trade secrets through internal misconduct, and obtained approval from management for both funding and implementation.

Measures Taken by Company G against Internal Misconduct

Purpose	Measure taken
To detect at an early stage access to trade secrets likely to result from employee misconduct	● Introduced a system in which real-time detection of what appears to be abnormal or non-routine access is possible
To preserve evidence of illegal access	● Took the advice of a forensic service provider to manage logs preserving evidence
To clarify that the information was leaked from the company	● Embedded digital watermarks into plans and documents involving trade secrets

In implementing preventative measures, the CISO saw to the following in particular.

- ● Referring to *サイバーセキュリティ関係法令 Q&A ハンドブック (Q&A Handbook on Cybersecurity Law)* by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), the CISO identified laws and regulations relevant to the protection of trade secrets and made certain that the planned measures did not conflict with them.
- ● When introducing continuous monitoring of access to trade secrets by employees (24 hours a day, 365 days a year), it was decided that the president would inform the entire company, specifically employees, that the purpose was to protect the company and its employees.
- ● Since in many cases involving internal misconduct at other companies the perpetrators thought they could remove the items in question without being noticed, at Company G, everyone with access to trade secrets was informed that multiple internal misconduct measures had been jointly introduced, so their removal would likely be detected at some point or other.
- ● There was also concern that internal communication problems could result in internal misconduct. To relieve this concern, it was decided that opportunities would be proactively created for supervisors and management to listen to employees' concerns and opinions.

Knowledge and Insight Gained

As with recent cyberattacks, information is leaked by insiders with an expectation for success. To deter this, it is important to make internal would-be perpetrators aware that all misconduct will eventually come to light. Therefore, Company G's CISO believes constant vigilance is required to maintain this awareness even in the face of future technological changes.