THE CYBER INVESTIGATIONS GUIDE

THIRD EDITION

Editors
Benjamin Powell and Shannon Togawa Mercer

The Cyber Investigations Guide

Third Edition

Editors

Benjamin A Powell

Shannon Togawa Mercer

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-253-6

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

Anderson Mōri & Tomotsune

BCL Solicitors LLP

Clifford Chance US LLP

Cravath, Swaine & Moore LLP

Jones Day

K&L Gates LLP

Nyman Gibson Miralis

Ropes & Gray LLP

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher's Note

The Cyber Investigations Guide is published by Global Investigations Review (GIR), the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature by providing an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its seventh edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation from discovery to resolution.

The Cyber Investigations Guide takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Cyber Investigations Guide* as the close-up.

The Cyber Investigations Guide is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

David Samuels
Publisher
May 2023

CHAPTER 11

Japan

Daisuke Yamaguchi, Takashi Nakazaki and Atsushi Nishitani[1]

Key cybersecurity standards and requirements

Notifications detailing mandatory cybersecurity standards have been issued by various government departments in Japan. For instance, the Ministry of Economy, Trade and Industries (METI) issued the Information Security Management Standards (the METI Standards) in 2003;[2] these were updated in 2016.[3] The METI Standards were formulated in accordance with international standards and practices. Furthermore, by incorporating the responses to opinions from external experts and public comments, among others, METI included the associated article numbers specified in ISO/IEC 27001,[4] added details to the simplified descriptions found in ISO/IEC 27001, and, by including other measures, the METI Standards were formulated so that they would contribute to the smooth operation of information security audit systems.

The METI Standards consist of two parts:

- management standards (based on JIS Q 27001:2014),[5] which provide for the ideal procedures for information security management – plan, do, check, act; and

1 Daisuke Yamaguchi and Atsushi Nishitani are partners and Takashi Nakazaki is a special counsel at Anderson Mōri & Tomotsune.

2 Ministry of Economy, Trade and Industries (METI), Public Notice No. 112 of 2003.

3 METI, Public Notice No. 37 of 2016.

4 The International Standard on requirements for information security management (jointly published by the International Organization for Standardization and the International Electrotechnical Commission).

5 ISO/IEC 27000:2014 provides the overview of information security management systems (ISMS), and terms and definitions commonly used in the ISMS family of standards. It was published in Japan as JIS Q 27001:2014.

- control measures standards (based on JIS Q 27001:2014 Appendix A and JIS Q 27002:2014), which provide for possible control measures to be implemented in establishing information security management.

In 2018, METI formulated two additional standards relating to cybersecurity: Information Security Service Standards and Standards for Examination-Registration Organizations for Information Security Services.

The Information Security Service Standards oversee:

- information security inspection;
- vulnerability diagnosis;
- digital forensics; and
- security monitoring and operation services.

The Information Security Service Standards stipulate a certain level of quality to be maintained in the respective services as regards:

- technical requirements (e.g., qualification requirements and explicit indication of specifications); and
- quality management requirements (e.g., allocation of quality control managers to appropriate duties, development of quality management manuals, and where service providers have introduced procedures for maintaining and improving quality).

Examination-registration organisations are bodies established to examine applicants as private information service providers, regarding whether or not the providers' services comply with the Information Security Service Standards, and to register appropriate providers. The Standards for Examination-Registration Organizations for Information Security Services stipulate rules that these organisations should observe, including fairness in examination and general rules for organisation management and examination procedures.

Sectoral standards

Telecommunications sector

The Ministry of Internal Affairs and Communications established the Safety and Reliability Standards of Information and Communication Network in 1987. These Standards have been amended several times and the latest version was released in 2020. The Security and Reliability Standards consist of two parts (facilities standards and management standards) and contain software measures, information security measures, earthquake countermeasures, power outage measures and various other measures.

Financial sector

The Financial Services Agency (FSA) issued a summary of its policies to strengthen cybersecurity in the financial sector in 2015 and updated it in 2018. The FSA plans to:

- promote continuous dialogue with financial institutions to understand their cybersecurity risks;
- improve information sharing among financial institutions;
- implement cyberattack drills in which financial institutions, the FSA and other public authorities participate; and
- develop human resources specialising in cybersecurity, and respond to new issues, such as accelerated digitalisation and international discussions.

The FSA's guidelines require banks to, among other things, establish an organisation to handle emergencies, designate a manager in charge of cybersecurity, prepare multi-layered defences against cyberattacks and implement a periodic assessment of cybersecurity.

Space systems sector

METI issued guidelines for cybersecurity measures for the civilian space systems sector in 2022. These have been updated in 2023.

Promotion of Economic Security Act

In February 2022, an expert panel set up to discuss economic security legislation released a 'Proposal on Economic Security Legislation'. In response to this, the Promotion of Economic Security Act (PESA) was enacted on 11 May 2022. The new Act introduced a system under which the government will conduct prior screening of infrastructure companies when they instal critical equipment (including systems) (to be applied by February 2024). The PESA requires that when 'specified social infrastructure business operators' intend to introduce critical facilities into essential business infrastructure or to outsource maintenance and management of critical facilities, they must first submit their plans to the government for examination. In general, the examination period is limited to 30 days but can be extended up to four months. During the examination period, operators are prohibited from introducing critical facilities into essential business infrastructure or outsourcing maintenance and management of critical facilities.

The specified social infrastructure business operators will be designated by the competent ministers from businesses that fall under any of the 14 infrastructure sectors, such as gas, oil, public transportation and finance. (See also the section titled 'Other important laws and regulations', below.)

Summary of breach notification rules

There are no general requirements for reporting security breaches under Japanese law; however, reporting requirements for breaches in the security of personal data were introduced under the Act on the Protection of Personal Information (Act No. 57 of 2003, as amended) (APPI) as of April 2022.

An amendment to the APPI in 2021 requires businesses to report to the Personal Information Protection Commission and notify data subjects who have suffered because of the breach when a business recognises that there has been, or might be, a security breach that is likely to 'harm the rights and interests of individuals'. Businesses will be required to report to the relevant authority within specified time frames and to inform affected individuals in a timely manner. Reporting will be required in the following circumstances:

1 leakage of special category data (similar to sensitive data);
2 damage to property, or potential risk of damage to property;
3 intentional violation of the law, such as unauthorised access; and
4 the breach affects at least 1,000 data subjects.

The amendment requires two stages of reporting. The first report must be submitted immediately after a breach occurs. The second report must be more detailed, and must be filed within 30 days of recognising any security breach as described in points (1), (2) and (4), above, and within 60 days of recognising any security breach as described in point (3). It should be noted, however, that when any of the situations described above arises, a business need not report a security breach to the Personal Information Protection Commission if it has implemented sufficient security management measures for protecting the rights and interests of individuals. A typical example of sufficient security management measures would be advanced encryption. This amendment came into effect on 1 April 2022.

There are specific reporting requirements in some business sectors, such as telecommunications and the financial sector.

The Telecommunications Business Act (Act No. 86 of 1984, as amended) (TBA), which is the main legislation governing that sector, requires a telecommunications carrier to report a security breach to a minister at the Ministry of Internal Affairs and Communication (MIC). Article 28 of the TBA specifies three specific events that must be reported:

1 when a telecommunications carrier suspends its telecommunications operations in part pursuant to the provisions of Article 8, Paragraph (2) of the TBA;
2 a violation of the secrecy of communications; or
3 any other serious accident specified by order of the MIC has occurred with respect to telecommunications operations.

In respect of point (2), above, many violations of the secrecy of communications cause a breach of personal data belonging to telecommunications service users. The reporting should be based on the guidelines on data breach reporting in the telecommunications sector, and should be carried out in accordance with the guidelines.[6] In respect of point (3), above, the relevant 'serious accidents' are specified in Article 58 of the Ordinance for Enforcement of the TBA. Details are available in the 'Guidelines for Application of the Telecommunications Business Act and Related Regulations on Telecommunications Accidents and Incidents'.[7] A telecommunications carrier is required to report an incident to the MIC promptly after its occurrence. In addition, the carrier is required to provide a detailed report of the incident to the MIC within 30 days of its occurrence. The report must include the following:

- the date and time of the incident;
- the date and time when the situation was remedied;
- the location of the incident (the location of the facilities);
- a summary of the incident and which services were affected by it;
- a summary of the facilities affected by the incident;
- details of the events or indications of the incident, the number of users affected and the affected service area;
- measures taken to deal with the incident, including the persons who dealt with it, in chronological order;
- causes that made the incident serious, including how the facilities have been managed and maintained;
- possible measures to prevent similar incidents from occurring;
- how the telecommunications carrier responded to enquiries from users and how it notified users of the incident;
- internal rules in connection with the incident;
- whether the telecommunications carrier has experienced similar incidents in the past, and a summary of those past incidents;
- the name of the manager of the telecommunications facilities; and
- the name and qualifications of the chief engineer of the telecommunications facilities.

6 www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/denkitsushin_rouei.html (in Japanese) (last accessed 26 April 2023).

7 www.soumu.go.jp/main_content/000743122.pdf (last accessed 26 April 2023).

As regards the financial sector, the FSA (the main authority responsible for supervising the financial sector) issues various guidelines for supervising financial organisations such as banks and insurance companies. For major banks, the FSA has issued 'Comprehensive Guidelines for Supervision of Major Banks, etc.' The Guidelines specify that the FSA requires banks to report a cybersecurity incident immediately after becoming aware of it. The report must include the following:

- the date and time when the incident occurred;
- the location of the incident;
- a summary of the incident and which services were affected by it;
- causes of the incident;
- a summary of the facilities affected by the incident;
- a summary of damage caused by the incident, and how and when the situation was remedied or will be remedied;
- any effect on other business providers;
- how the bank responded to enquiries from users and how it notified users, public authorities and the general public; and
- possible measures to prevent similar incidents from occurring.

The government encourages each business industry to share security information among the relevant industry groups. Apart from reporting to the authorities, there are many information-sharing and analysis centres (ISACs) in various business sectors, including the financial sector and the information and communication technology sector.[8] Several business sectors have established ISACs and encourage the relevant industry members to share security information with them. For example, Financials ISAC Japan has two core functions:

- collective intelligence, which focuses on intelligence sharing between members in relation to any daily incident or exposed vulnerability; and
- resource sharing, which, through cooperative action, pools resources to promote consideration of strategies to deal with shared issues.

Financials ISAC Japan has more 400 financial institutions as regular members and around 30 information technology vendor companies as affiliate members. Financials ISAC Japan holds cyberattack drills regularly. If it finds important

8 Many information sharing and analysis centres (ISACs) have been established, such as Financials ISAC Japan, ICT ISAC Japan, Japan Automobile ISAC, Software ISAC and Japan Electricity ISAC.

information, 100 members will be committed to conducting a variety of activities with the aim of building a solid foundation to promote customers' peace of mind, safety and security, which lie at the heart of Japan's financial system.

Best practices for responding to a cyber incident

Cybersecurity Management Guidelines Version 3.0, issued by METI in March 2023, sets out best practices for responding to a cyber incident. The Guidelines stipulate that it is important to develop a cybersecurity incident response team, and that relevant procedures should be put in place to establish a response structure within the organisation (such as a computer security incident response team (CSIRT)) to identify the scope of impact and damage; to take initial action to prevent further damage and implement measures to prevent similar incidents from recurring; to decide what information should be reported to whom in the event of an emergency; and support management to report that information to internal and external stakeholders appropriately.

The following is a checklist for recommended best practices:

- Conserve evidence about the various logs and devices infected with malware following a cyberattack, for swift identification and analysis of the cause of damage, and give directions to employees to cooperate with relevant organisations for joint investigation. When investigating the cause of an incident, the Guidelines recommend referring to Appendix C thereof – 'Items to organise within the organisation for the occurrence of incidents'.
- Execute drills in preparation for cyberattacks, including developing measures to prevent similar incidents from occurring and reporting to relevant government agencies. The Guidelines recommend considering consulting external experts as necessary for measures to prevent recurrence.
- Prepare a list of emergency contacts (security vendors, etc.) and a list of organisations to which to disclose information, including external parties, and share those lists with incident response members.
- Calculate the impact of first response on regular business operations and, based on that, make arrangements in advance with other divisions of the organisation (human resources, sales, etc.) for emergencies.
- Check relevant laws and regulations and procedures to fulfil obligations described therein.
- Report to management the damage status and impact on other companies as a result of an incident.

Cybersecurity and incident response trends

Increasing number of cybersecurity incidents

As in many other countries, the number of cyberattacks in Japan continues to rise. According to the National Police Agency, it received reports of 230 cases of ransomware damage in 2022 (a 57.5 per cent increase from 2021), a number that has been rising steadily since the second half of 2020.[9] The number of phishing incidents reported to the Council of Anti-Phishing Japan was 526,504 in 2021, which is 2.3 times more than in 2020.[10]

In December 2020, METI issued a news release, warning that:

- there had been a rapid expansion of diversity of cyberattack patterns targeting supply chains in which small and medium-sized enterprises (SMEs) are involved;
- there had been a rapid increase in the number of ransomware victims, regardless of the size of the enterprise; and
- overseas connections were becoming targets of attackers wishing to steal highly sensitive information.[11]

Challenges in Japan

One of the most crucial issues in cybersecurity areas is the shortage of cybersecurity professionals. According to a research report,[12] 86.2 per cent of Japanese companies think they do not have enough human resources for cybersecurity, compared with 16.1 per cent of US companies and 17.1 per cent of Australian companies. Another research report[13] showed that only 22.8 per cent of Japanese companies (from 534 samples) have at least one full-time CSIRT member.

---

9 National Police Agency, 'Threats to Cyberspace in 2022' (16 March 2023) (https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf (in Japanese) (last accessed 3 May 2023)).

10 Council of Anti-Phishing Japan, 'Phishing Report 2022' (1 June 2022).

11 'Alerts to Company Executives to be Issued to Encourage them to Enhance Cybersecurity Efforts in Light of Situations of Recent Cyberattacks' (18 December 2020) (www.meti.go.jp/english/press/2021/1218_001.html (last accessed 26 April 2023)).

12 NRI SecureTechnologies, Ltd, 'NRI Secure Insight 2020' (published 15 December 2020) (https://www.nri-secure.co.jp/download/insight2020-report (in Japanese) (last accessed 26 April 2023)).

13 Information-technology Promotion Agency, 'Report on survey of CISO, etc. and promotion of security measures of companies' (25 March 2020) (https://www.ipa.go.jp/archive/security/reports/2019/ciso.html (in Japanese) (last accessed 3 May 2023)).

Lack of cybersecurity professionals causes various problems for Japanese companies and sometimes prevents them from quickly identifying, responding to and recovering from cybersecurity issues.

Regulatory consideration

Legal framework

The Basic Act on Cybersecurity (Act No. 104 of 2014, as amended) (BAC), which came into effect in January 2015, was the first statute focusing on cybersecurity issues. The BAC provides the basic framework of government policies for cybersecurity, including basic principles, responsibilities of the Japanese government and local governments, and essential matters for cybersecurity-related policies.

The Cybersecurity Strategy of the Japanese government is determined and published pursuant to the BAC; however, the BAC is not intended to regulate the activities of private companies and individuals directly. Concurrent with enforcement of the BAC, the Cybersecurity Strategic Headquarters (CSH) and National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) were established by the Cabinet of Japan to promote various cybersecurity-related policies and coordinate with various stakeholders in both the public and the private sectors.

Specific regulations and legal responsibilities regarding cybersecurity issues are stipulated in individual laws and regulations. The following are important laws regarding cybersecurity in Japan.

Personal Data Protection Regulations

The APPI regulates the handling of personal data mainly in private sectors. It requires business operators that handle personal information to take necessary and appropriate action for controlling the security of personal data, including preventing leaks, loss or damage of the personal data it handles. The Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013, as amended) (the My Number Act) also requires those responsible for handling 'Individual Numbers'[14] to adopt necessary measures to ensure the appropriate management of Individual Numbers, such as preventing leaks, loss or damage of Individual Numbers. Under the amendment to the APPI

14 The Individual Number (My Number) is a unique 12-digit number for each individual provided by the government, and used in social insurance, tax and disaster countermeasure areas within Japan.

enacted in 2021, the obligation to notify the Personal Information Protection Commission (PPC) of a personal data breach has been in force since April 2022. Violations of this obligation may result in penalties.

The main regulator for the APPI and the My Number Act is the PPC, the independent regulatory body established based on the APPI. It is responsible for establishing the Basic Policy on Protection of Personal Information and overseeing compliance with the APPI and the My Number Act. The PPC has issued detailed guidance on the scope and interpretation of the APPI. In addition, relevant administrative authorities have also issued guidelines for specific areas, including the finance, medical, telecommunications, employment and welfare sectors. Although these guidelines are not legally binding, they are generally accepted by companies and legal practitioners.

Other important laws and regulations

Under the Companies Act (Act No. 86 of 2005, as amended), it is understood that directors of a Japanese company have a duty to establish appropriate cybersecurity measures as part of the company's internal control system. Breach of this duty could result in civil liability (including a shareholder derivative suit) against directors.

In connection with the management of cybersecurity by companies, METI and the Information-technology Promotion Agency jointly published the Cybersecurity Management Guidelines in 2015, which were revised (Version 2.0) in 2017.[15] These Guidelines are aimed at the corporate management of major companies as well as SMEs and include, from the viewpoint of protecting companies from cyberattacks, the three principles that management need to recognise and 10 important items that management should direct their executive in charge to observe in implementing cybersecurity measures. The Guidelines themselves are not legally binding, but whether they are followed or not may be an important factor to consider as regards directors' compliance with their duties (see the section titled 'Litigation consideration', below, for details).

For the telecommunications sector, the TBA requires telecommunications carriers to maintain telecommunications facilities that conform with the technical standard specified by the Order of the Ministry of Internal Affairs and

15 www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf (last accessed 26 April 2023).

Communications, which includes detailed cybersecurity-related requirements. From April 2020, certain security measures for internet of things devices have been included in the technical standards.

As to criminal liability, the Act on Prohibition of Unauthorised Computer Access (Act No. 128 of 1999, as amended) prohibits unauthorised access to computer systems, as well as the illegal collection of identity documents and passwords of other people and provision thereof. Violators could face up to three years in prison or a ¥1 million fine.

The Unfair Competition Prevention Act (Act No. 47 of 1993, as amended) and Copyright Act (Act No. 48 of 1970, as amended) prohibit the provision of software or devices exclusively for the purpose of circumvention of technological restriction or protection measures (i.e., copy control or access control measures). Violators could face up to three years in prison or a ¥3 million fine under the Copyright Act, or up to five years in prison or a ¥5 million fine, or both, under the Unfair Competition Prevention Act. Acquisition of a trade secret by an act of fraud (including unauthorised access as stipulated in the Act on Prohibition of Unauthorised Computer Access) shall be subject to up to 10 years in prison or a ¥10 million fine, or both.

The Penal Code (Act No. 45 of 1907, as amended) also prohibits certain cyberattack-related activities, including:

- making or distributing computer viruses (up to three years in prison or a ¥500,000 fine);
- skimming credit card information (up to three years in prison or a ¥500,000 fine);
- obstructing the business of another by interfering with the operation of a computer or damaging an electromagnetic record (up to five years in prison or a ¥1 million fine); and
- computer fraud by creating a false electromagnetic record, inputting false data or giving unauthorised commands (up to 10 years in prison).

In light of the increasing number of cyberattacks that appear to be coming from overseas, the PESA introduced a new rule under which the government will conduct prior screening of infrastructure companies when they instal critical equipment (including systems). This new rule is scheduled to be in effect by February 2024. The outline of this rule is as follows:

- the government designates eligible business operators;

- the eligible business operators must, in principle, notify the government in advance if they intend to do any of the following:
  - instal critical facilities (such as hardware and software, including where they are provided by cloud services); or
  - outsource the maintenance, management or operation of critical facilities to another entity;
- when an advance notification is submitted, the government shall examine whether there is a significant risk that the critical facilities will be used to sabotage the stable provision of core infrastructure services from outside the country; and
- if, as a result of the examination, the government determines that there is a significant risk that the critical facilities will be used for sabotage from abroad, it may recommend or order a change in the method of installation, etc. or discontinuation of the installation.

The eligible business operators (specified social infrastructure business operators) will be designated by the competent minister from among 14 infrastructure business sectors (including electricity, gas, oil refining, water, railroad, cargo, air transport, airport, telecommunications and broadcasting) that meet certain conditions.

Cybersecurity regulators

As the CSH and NISC are mainly responsible for strategy planning and coordination, there is no one-stop regulator on cybersecurity matters in Japan. The PPC is the main regulator of data protection issues and has the authority to provide guidance and advice, request reports, conduct on-site inspections, offer recommendations, and give orders to government institutions and business operators who handle specific personal information. For other specific areas and industries, the ministry with jurisdiction over the applicable laws and regulations should be the main regulator (for example, the MIC for telecommunications business).

Litigation consideration

A company that has suffered a cyberattack may be sued by an affected business partner or individual, or a lawsuit may be instituted by a shareholder against the company's directors and officers.

Suit against a company by a business partner or individual who has suffered damage

Claim for damages based on breach of contractual provisions

As an example, a business partner enters into a business alliance agreement with Company A and discloses confidential information (technical information, customer information, etc.) to Company A. If that information is stolen as a result of a cyberattack by a foreign hacker on Company A's systems, and the business partner suffers damage as a result, the business partner may file a claim for damages against Company A based on the breach of contractual provisions (i.e., breach of obligations to safeguard and protect the business partner's confidential information, obligations for secure management of information, etc.).

Under the Civil Code of Japan, to establish breach of contract, one must prove:

- the fact that there was a default by a party;
- the reasons for which the defaulting party is to be held responsible; and
- the damage caused (Civil Code, Article 415).

The quantum of damages that can be claimed will depend on the limitation on the compensation for damages agreed by both the parties in the contract. However, in the absence of such a limitation clause, in addition to ordinary damages, special damages that could have been foreseen at the time of the default are also covered under the Civil Code (Article 416, Paragraph 2).

Therefore, in addition to the damage arising from the theft of technical information, in the event that the level of sales of the products using that technical information falls, Company A will be liable to compensate the business partner for the decrease in sales as special damages.

Claim for damages based on tort

If an individual's personal information is stolen from a company and there is no contractual relationship between the individual and the company, the individual may file a claim under tortious liability against the company.

The facts required for claiming damages based on tort are intention and negligence, illegality (infringement), damage and causality (Civil Code, Article 709).

Unlike in the United States, it is not possible to claim for punitive damages in Japan.

Suit instituted by shareholders against directors and officers

If a company suffers damage as a result of a cyberattack that has occurred because of insufficient cybersecurity systems being put in place to protect confidential data, shareholders may institute a derivative suit against the company's directors and officers for breach of their duty of care.

At present, there have been no cases of shareholders' lawsuits being instituted for damages owing to a failure to provide cybersecurity systems in Japan. However, with regard to theft of personal information, the Benesse Group experienced a personal information leak: an employee of a business operator entrusted with the management of personal information of customers illegally acquired or sold personal information. A shareholder lawsuit was instituted against the director of a holding company of the Benesse Group, for compensation of ¥26 billion.

Rejecting the appellant request of the shareholders, the appeals court found that:

- the Benesse Group had established various rules (such as the Business Corporation Management Rules) and, based on these, conducted a certain level of business management through participation in personnel affairs and business planning, risk assessment and examination of the group as a whole, reading of various reports, among other things, to ensure compliance with laws and regulations, and established and operated an internal control system as a group of companies; and
- there was no proof that, considering the practice of domestic listed companies at the time of this case, the establishment and operation of the Benesse Group's internal control system was below the required standard.[16]

As can be seen from this case, the establishment of a system to protect personal information or to promote cybersecurity constitutes a part of the duties of directors to establish and operate internal control systems.[17]

The three principles and the 10 important items set forth in the Cybersecurity Management Guidelines represent a specific model of the philosophy and measures of the internal control system that should be established in relation to a cybersecurity system. To prevent directors from being sued for violation of their managerial obligation of due care, it is necessary to establish and check the

16 Appeal court decision by the Okayama branch of the Hiroshima High Court, 18 October 2019.

17 Companies Act, Article 348, Paragraph 3, Item 4.

cybersecurity system of the company, and to establish a system that does not fall below the standard of current practice as mentioned above, especially pertaining to the above three principles and the 10 important items.

Types of threats or threat actors

Criminals (hackers), the state and insiders (whether the action is intentional or accidental) are considered to be the main actors who conduct cyberattacks.

Offender

Cybercriminals in Japan engage in illegal information access or theft of company assets through methods such as malware attacks, ransomware attacks, denial of service, distributed denial of service, phishing emails, business email fraud and unauthorised access or alteration of websites.

In 2015, the terminals of employees of the Japan Annuity Payments Organization were illegally accessed by means of sending an email with a virus from outside, targeting the organisation: 1.25 million people's personal information (basic pension number, name, date of birth and address) were leaked.

Nation

In the *Coincheck* incident, about ¥58 billion worth of the virtual currency NEM was stolen in January 2018.[18] The breach was carried out by an overseas hacker. Coincheck put the 'private key' used for transactions, such as remittance of virtual currency, in a hot wallet connected to the internet (a wallet disconnected from the internet is called a cold wallet). The private key was allegedly stolen by an outside hacker through the internet, and a large number of NEMs were stolen. The NEM Foundation, in cooperation with engineers, placed tracking mosaics on the stolen NEM wallets, keeping them under constant surveillance to prevent perpetrators from converting the stolen NEMs into other currencies. However, even with this tracking method, if the perpetrator exchanged the NEMs for another currency in the highly anonymous network called the Dark Web, identification of the perpetrator who stole the NEMs would be extremely difficult.

18 See, e.g., https://www.bbc.co.uk/news/world-asia-42845505 (last accessed 26 April 2023).

Insiders

Damage incurred by a company may be caused by intentional fraud or human error by an insider. Typical examples of insider fraudulent activities are as follows:

- employees send important information to personal addresses with email attachments;
- employees use apps installed on company-leased smartphones to connect to the company's computer and take confidential information outside using Wi-Fi;
- removal or exchange of confidential information by a system administrator;
- leakage of customer information by an outsourced employee;
- removal or exchange of confidential information by a homeworker;
- removal of confidential information by retirees; and
- actions that are not intentional, for example, when a leak of personal information is caused by human error, such as inadvertent erroneous transmission of emails.

Damage suffered by a company as a result of fraud by insiders include the loss of customer information, business information and technical information that the company manages as its trade secret; economic loss resulting from liability for damage to customers; and reputational damage resulting from loss of credibility as a company.

Recent trends in types of cyberthreat and detection times

Because hacking from overseas was raised as a possibility with regard to the *Coincheck* incident (see above), administrative supervision and legislation in Japan alone cannot adequately deal with such an incident. The Financial Stability Board, which comprises financial supervisory authorities in major countries, created a contact list to help local authorities in charge of virtual currency administration in each country to understand their responsibilities. In addition, if any cybercrime actually occurs, a system must be established to identify the culprit through international cooperation among investigative authorities and engineers in each country, and to investigate and recover assets outside Japan.

As part of international cooperation, METI signed a Memorandum of Cooperation on Cybersecurity with the US Department of Homeland Security on 6 January 2023.