Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2024

Definitive global law guides offering comparative analysis from top-ranked lawyers

Japan: Trends & Developments

Yasushi Kudo
Nagashima Ohno & Tsunematsu

JAPAN

Trends and Developments

Contributed by:
Yasushi Kudo
Nagashima Ohno & Tsunematsu

Nagashima Ohno & Tsunematsu is one of the foremost providers of international and commercial legal services, based in Tokyo. The firm has over 550 lawyers, including nearly 50 experienced foreign lawyers from various jurisdictions. Its overseas network includes offices in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi and Shanghai, and collaborative relationships with prominent local law firms throughout Asia, Europe, North and South America, and other regions. The firm provides comprehensive assistance in the development of cybersecurity systems, including the establishment of internal governance systems and vendor management. It also has extensive experience in crisis management in the event of a security incident. In collaboration with IT system experts, Nagashima Ohno & Tsunematsu also provides one-stop support for the entire process, from the initial response, including fact-finding and evidence preservation, to dealing with the authorities, information disclosure and the mass media, handling victims, root cause analysis and recurrence prevention measures.

Author

Yasushi Kudo is a partner at Nagashima Ohno & Tsunematsu. He mainly focuses on crisis management, including dealing with domestic and international authorities, regulatory compliance, cybersecurity/data privacy, and advice on compliance systems and corporate governance, leveraging his expertise and experience gained from secondment to the Financial Services Agency and the Securities and Exchange Surveillance Commission. Recently, he has focused on legal issues raised by cybersecurity incidents such as ransomware attacks, data compromise and business e-mail compromise, as well as the development of internal control systems so as to mitigate cybersecurity risks such as supply chain risk.

Nagashima Ohno & Tsunematsu

JP Tower
2-7-2 Marunouchi
Chiyoda-ku
Tokyo 100-7036
Japan

Tel: +81 3 6889 7396
Fax: +81 3 6889 8396
Email: yasushi_kudo@noandt.com
Web: www.noandt.com/en/lawyers/yasushi_kudo/

Cybersecurity Law in Japan in 2024

Introduction

In light of the escalating cyber threats in Japan during the year 2023, as reported by the Japanese National Police Agency (JNPA), it has come to the attention of the authorities that certain cyber attacks were perpetrated by hackers believed to be aligned with Russia, influenced by the ongoing Ukrainian conflict. Furthermore, the JNPA's report underscores the persistent prevalence of ransomware attacks, with a noteworthy increase in incidents related to a new form of ransomware known as "No-ware ransom." This variant involves the theft of data from victims' companies without encrypting the information, thereby causing substantial harm. Additionally, the Information-technology Promotion Agency (IPA) publicly reported "10 Major Security Threats 2024". In this article, concerning threats to enterprises, attacks exploiting vulnerabilities embedded in the supply chain is ranked second, while damages caused by ransomware attacks is ranked first.

Given the concerning trend in cyber attacks, the Japanese government, along with pertinent government agencies, has proactively revised and released updated guidelines for enhancing cybersecurity risk management, including supply chain risk management. This revision is aimed at fortifying the nation's resilience against cyber threats and ensuring a comprehensive response to emerging challenges.

The subsequent sections provide an in-depth examination of the specific circumstances surrounding the cyber attacks in Japan during 2023. Additionally, a detailed elucidation is presented of the modifications made to existing systems and the guidelines issued by the Japanese authorities in response to these circumstances. This comprehensive overview serves to articulate the evolving landscape of cybersecurity in Japan and the corresponding measures, especially in relation to the supply chain risk management implemented to safeguard national interests.

Cybersecurity incidents in Japan

In September 2023, JNPA disseminated a report titled "Regarding the Circumstances of Threats in Cyberspace from January to June 2023."

This publication highlights instances of website disruptions attributed to Distributed Denial of Service (DDoS) attacks during the aforementioned period. Notably, certain hacktivist groups aligned with the Russian government asserted their involvement in these incidents through messages posted on social media platforms.

The report also underscores that ransomware attacks remained prevalent, with 103 documented cases during the specified period, signifying a sustained high level of threat. Of particular concern are 65 instances of double extortion, wherein companies faced threats of public data disclosure unless a ransom was paid. Among these, 22 cases involved direct payment requests from the attackers, with 21 of them specifying cryptocurrency as the preferred form of payment. The JNPA identified a new modus operandi termed the "No-ware ransom" case, wherein attackers pilfered data without encryption and demanded payment.

Additionally, the report reveals a continuation of the trend observed in 2022, wherein cybercriminals exploited vulnerable VPN devices and weak credentials in remote desktop services as a conduit for ransomware attacks.

A granular examination of the 103 ransomware cases indicates 30 instances targeting large enterprises and 60 affecting small and medium sized enterprises. Furthermore, the breakdown by industrial categories reveals 34 cases in manufacturing, 16 in services, and 15 in wholesaling and retailing. Consequently, the pervasive impact of ransomware attacks is evident across industries, irrespective of size or sector.

Moreover, in January 2024, IPA publicly reported "10 Major Security Threats 2024". Every year, IPA evaluates ten major threats to individuals and enterprises. Concerning threats to enterprises, attacks exploiting vulnerabilities embedded in the supply chain is ranked second, while damages caused by ransom attacks is ranked first. This result is the same as in "10 Major Security Threats 2023".

Revised Cybersecurity Management Guideline announcement by the Ministry of Economy, Trade and Industry and Information-technology Promotion Agency

In March 2023, the Ministry of Economy, Trade and Industry (METI) and IPA jointly revised the Cybersecurity Management Guidelines (CMG). The CMG establishes that companies bear the responsibility for mitigating cybersecurity risks to an acceptable level.

The CMG outlines the following key components:

- Three management principles:
  - (a) Management must acknowledge cybersecurity risks as critical elements in the company's risk management and spearhead countermeasures.
  - (b) Management, to fulfil its cybersecurity responsibilities, should extend attention to cybersecurity measures across the entire supply chain, including domestic and overseas bases, business partners, and contractors.
  - (c) In both normal and emergency situations, management must actively communicate with relevant parties to effectively implement cybersecurity management.
- Ten key items of cybersecurity management – management is instructed to involve executives (including the Chief Information Security Officer) in key aspects, such as identifying

cybersecurity risks, establishing organisation-wide policies in response to these risks, and constructing a robust system for cybersecurity risk management.

The current revision of the CMG takes into consideration the evolving circumstances in Japan, including:

- The widespread adoption of remote work and the diversified nature of work, founded on a digital environment.
- The expanded impact of ransomware attacks, causing disruptions to corporate activities.
- The growing need to propagate cybersecurity measures throughout the entire supply chain due to the increasing spread of cybersecurity-related damage across domestic and international supply chains.
- Heightened investor interest in companies' endeavours to enhance corporate governance and enterprise risk management, driven by the surge in Environmental, Social, and Governance (ESG) investments.

Significant alterations in the CMG include the emphasis on implementing measures throughout the entire supply chain, acknowledging the escalating cyber threats through supply chain channels.

In October 2023, METI and IPA jointly released a compendium of best practices aligned with the revised CMG, providing practical guidance for the application of principles and instructions outlined in the guidelines. This initiative aims to assist companies in enhancing their cybersecurity posture in line with the latest CMG revisions.

Guidelines for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure and Risk Management Guidelines for the Department in Charge of Cybersecurity in the Critical Infrastructure Operator in Accordance with the Cybersecurity Policy for Critical Infrastructure Protection

Introduction to Cybersecurity Policy for Critical Infrastructure Protection

In June 2022, the Cybersecurity Strategic Headquarters Government of Japan (CSH) unveiled the Cybersecurity Policy for Critical Infrastructure Protection (CPCIP). Aligned with the cybersecurity strategy stipulated in the Basic Act on Cybersecurity, CPCIP aims to encourage Critical Infrastructure (CI) operators to enhance cybersecurity assurance among them.

CPCIP delineates the responsibilities of the state, local authorities, Chief Information Officers (CIOs) within CI operators, and cybersecurity-related projects. Its objective is to ensure the secure and sustained provision of CI services. Recognised as a critical management concern, CPCIP actively promotes the fortification of incident response systems in CI operators during cybersecurity-related security incidents. Moreover, CPCIP asserts that an organisation's cybersecurity structure is integral to its internal control system, suggesting that compliance with the duty of care under the Companies Act may necessitate appropriate cybersecurity measures.

CPCIP categorises the following 14 sectors as CI.

- Information and communication.
- Financial services.
- Aviation.
- Airports.
- Railways.

- Electric power supply.
- Gas.
- Government and administrative services.
- Medical.
- Water supply.
- Logistics.
- Chemical industry.
- Credit cards.
- Petroleum.

In light of a cyber-attack case leading to the unauthorised disclosure of a substantial amount of customers' personal information, the Okayama Branch of the Hiroshima High Court in a ruling on 18 October 2019 elucidated the directors' duty of care under the Companies Act. The court affirmed that the adequacy of internal control systems is determined by industry practices, and its specific content is contingent on the discretion of directors, considering factors such as the business, size, and management status of the company or group in question.

The court's judgment is considered valuable when assessing the directors' duty of care concerning the internal control system in response to cybersecurity.

CPCIP illustrates specific guidelines as to actions to be carried out by CI operators. The key areas of focus include:

- strengthening cybersecurity incident response systems;
- development and penetration of safety principles;
- reinforcing information-sharing systems with cybersecurity-related organisations;
- utilising risk management; and
- enhancing the protection infrastructure.

Outline of Guidelines for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure

- In July 2023, CSH released the Guidelines for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure (GESP), building upon CPCIP.
- Objectives and structure – GESP, aligned with CPCIP, underscores the importance of clearly presenting cybersecurity measures in "Safety Principles" comprehensible to all stakeholders involved in CI businesses.
- Classification of safety principles – GESP categorises "Safety Principles" into four distinct categories:
  (a) Mandatory standards, stipulated by the government based on relevant laws.
  (b) Recommended standards and guidelines, articulated by the government in accordance with relevant laws.
  (c) Industry standards and guidelines, cutting across various sectors, formulated by industrial organisations to meet citizen expectations and comply with relevant laws.
  (d) Internal regulations, established by CI operators to fulfil the expectations of citizens, users, and relevant laws.
- Utilisation of risk management and crisis management – GESP emphasises the inclusion of specific items in Safety Principles to enable organisations to:
  (a) Conduct self-evaluation of the current implementation status of cybersecurity measures.
  (b) Analyse deviations from the ideal situation and requirements.
  (c) Prioritise inadequate measures based on the analysis results.
  (d) Implement specific measures.
- Supply-chain threats and risk management – GESP identifies representative threats to the supply chain, including:

(a) Embedding of unauthorised functions.
(b) Service disruption in the supply chain.
(c) Inappropriate handling of information in external services.
(d) Cyber-attacks originating from overseas bases, group organisations, and business partners.

- For supply-chain risk management, GESP prescribes the following measures:
  (a) Conduct risk assessments and responses specific to supply-chain risks.
  (b) Adhere to local laws, regulations, and cultural considerations with respect to overseas bases.
  (c) Clearly define roles and responsibilities in contracts between business operators and direct suppliers to address cybersecurity risks.
- Desirable measures for supply-chain risk management – GESP recommends the following measures to enhance supply-chain risk management:
  (a) Conduct comprehensive risk management of the entire supply chain by assessing the involvement of suppliers linked to direct suppliers, based on risks.
  (b) Facilitate each supplier's understanding of the implementation status of risk management in suppliers located upstream.
  (c) Strengthen the overall effectiveness of supply-chain measures through support for the introduction of security measures and collaborative implementation.

GESP serves as a comprehensive guide for CI operators, offering a structured approach to cybersecurity measures and risk management principles in accordance with the evolving threat landscape outlined in CPCIP.

Outline of Risk Management Guidelines for the Department in Charge of Cybersecurity in the Critical Infrastructure Operator

- In July 2023, the National Center of Incident Readiness and Strategy for Cybersecurity released the Risk Management Guidelines for the Department in Charge of Cybersecurity in the Critical Infrastructure Operator (RMG) to elucidate essential processes and security measures for leveraging risk management and crisis management, as outlined in GESP.
- Objectives and structure – RMG aims to provide a comprehensive framework for the effective utilisation of risk management and crisis management, with a focus on key processes and security measures prescribed in GESP.
- Supply-chain risk management measures – among other things, RMG delineates specific measures for supply-chain risk management, encompassing various aspects:
  (a) Organisation of requirements for cybersecurity upon the procurement and use of products and services.
  (b) Management of risks caused by embedding of unauthorised functions, etc.
  (c) Inclusion, in the selection criteria, of matters ensuring consistent quality control in the procurement process.
  (d) Establishment of an inspection system to verify the implementation of specified security requirements and detect illegal programs.
  (e) Confirmation of the contractor's ability to supervise subcontractors and assume liability for results caused by such subcontractors.
  (f) Prohibition of re-entrustment, or inclusion of the requirement for prior permission by a principal in the contract.
  (g) Management of risks from service disruption:

(i) Consideration of continuous provision of parts by suppliers or of alternative measures.
(ii) Confirmation of the supplier's business plan and performance of provision.
(iii) Verification of the site where the contractor implements its project and assessment of location conditions.

(h) Management of risks from inappropriate handling of information:
(i) Selection of reliable services.
(ii) Implementation of confirmation measures to ensure proper return or deletion of information.

(i) Management of risks from cyber-attacks via overseas entities:
(i) Use of verification results by a third-party.
(ii) Verification of cybersecurity at the point of network connection to the supply chain.

The RMG serves as a valuable resource for the department in charge of cybersecurity in CI operators, offering practical guidance to enhance the robustness of risk management practices, including supply-chain risk management, within the broader context of cybersecurity.

Outline of the System for Ensuring Provision of Essential Infrastructure Services under the Economic Security Promotion Act

- Introduction – the Economic Security Promotion Act (ESPA), enacted in 2022 in response to escalating cybersecurity threats in Japan, establishes the system ("System") for Ensuring Provision of Essential Infrastructure Services (EIS). This system, operational from May 2024, aims to mitigate risks such as the embedding of malware during equipment installation or software updates and the exposure of vulnerability information in facilities by third parties outside Japan.
- Development of Guidelines – in 2023, competent authorities crafted guidelines to prepare for the effective implementation of the System beginning in 2024.

Outline of the System for Ensuring Provision of EIS

- Purpose – the primary objective of the System is to prevent critical facilities of the EIS (CF) from being exploited as a means of disrupting stable provision of the EIS from outside Japan. Competent authorities conduct a prior screening process and issue recommendations or orders concerning the installation or entrustment of maintenance, etc, of the CF.
- Scope of the EIS – the EIS encompasses services in electricity, gas, oil, water, railways, truck transport, international maritime cargo, aviation, airports, telecommunications, broadcasting, postal services, financial services, and credit cards. Designated as EIS are services that are either (i) crucial for national livelihoods or economic activities and the lack of which may lead to widespread or large-scale social turmoil or (ii) essential for citizen survival with limited substitution possibilities. Competent authorities in the respective EIS fields designate the specific services falling under this purview. Please be informed that, in response to a ransom-ware attack to the Nagoya United Terminal system operated in Nagoya port facilities in July 2023, as a result of which certain port-facility operations were suspended for a couple of days, the Japanese government decided to amend the relevant regulations in order to add "port transport" to the EIS in January 2024.
- Scope of the CF – critical to the stable provision of EIS, equipment or programs that may be exploited for interference with the stable provision of EIS, such as through cyber-attacks or physical interception measures, are

designated as CF. Competent authorities in the respective EIS fields identify and designate such CF.
- Scope of the EIS operators – EIS operators are designated based on the unique circumstances of each EIS, considering factors such as the scale of operation or substitutability. Competent authorities in the respective EIS fields identify and designate EIS operators.
- Duty of the EIS operators – upon the installation of CF for business use or the commencement of entrustment of maintenance, etc, of CF to other business operators, EIS operators are generally required to submit a plan in advance and undergo a screening process conducted by the competent authorities. This measure ensures a proactive approach to cybersecurity, aligning with the overarching goals of ESPA.

The outlined System under ESPA establishes a comprehensive framework to fortify the cybersecurity posture of CF, safeguarding against external threats and disruptions to the EIS.

Outline of the Prior Screening Process in the System for Ensuring Provision of Essential Infrastructure Services under the Economic Security Promotion Act

- Introduction – the prior screening process is a crucial component of the System under the ESPA. It involves a proactive approach by EIS operators, which are required to notify the competent authorities of their plans for the installation or entrustment of maintenance, etc, of CF and undergo a review process.
- Prior notification plan:
  - (a) Installation:
    - (i) Summary of critical facilities, including content, timing, suppliers, components, etc.
    - (ii) Measures for managing risks related to installation.
  - (b) Entrustment of maintenance, etc:
    - (i) Summary of critical facilities, including content, timing, contractors, subcontractors, etc.
    - (ii) Measures for managing risks related to the entrustment of maintenance, etc.
- Measures for risk management:
  - (a) The EIS operator is required to report the measures taken to prevent interference with CF in both types of notifications.
  - (b) Relevant laws and subordinate regulations provide a list of items to be implemented by the EIS operator.
  - (c) Specific examples of measures are outlined in the System's guidance.
- Examples of detailed measures:
  - (a) For installation:
    - (i) Conduct necessary controls to prevent unauthorised changes to the CF and their components during manufacturing by suppliers. A contract should stipulate the EIS operator's right to verify these controls.
    - (ii) Selection of suppliers considering future maintenance and inspection needs for the CF and their components.
    - (iii) Adoption of a system to identify signs of unauthorised disruption of the CF and their components, as a result of which the provision of the EIS can be maintained.
  - (b) For entrustment of maintenance, etc:
    - (i) Implementation of necessary controls to prevent unauthorised changes to the CF by the entrusted party (including the re-entrusted party). A contract should allow the EIS operator to verify such controls.
    - (ii) In the case of re-entrustment, a contract should stipulate the provision of information for cybersecurity checks and approval by the EIS operator.

(iii) Verification by the EIS operator to ensure the entrusted party does not discontinue or suspend services in violation of the contract.

(c) For both installation and entrustment:

(i) Verification of compliance with Japanese laws and internationally accepted standards by suppliers and maintenance counterparts.

(ii) Confirmation that foreign legal environments do not affect the CF and the supply of components thereof, or the appropriateness of maintenance, etc, of the CF entrusted (including any re-entrusted part).

(iii) Inclusion of clauses in contracts for the provision of information on external influences to which the suppliers and the entrusted parties are subject, including re-entrustment and timely updates.

- Flexibility in implementation:
  - (a) The Japanese government acknowledges that measures should be determined based on the nature and degree of risk associated with the business.
  - (b) EIS operators are not obliged to implement all listed measures; they can choose substantially equivalent measures and select relevant items accordingly.
  - (c) The focus is on achieving the intended cybersecurity goals, allowing flexibility in implementation based on individual circumstances.

This outlined process ensures that EIS operators actively engage in risk management and cybersecurity measures, fostering a collaborative effort with competent authorities to protect the CF from external threats. In addition, the examples of detailed measures for risk management serve as a valuable resource not only for the EIS operators but also for other business operators to establish and promote supply-chain risk management, and to mitigate risks resulting in breach of the directors' duty of care concerning the internal control system in response to cybersecurity.

- Screening period:
  - (a) The competent authorities will review the content of the prior notification.
  - (b) In principle, the screening period is within 30 days from the receipt of the plan by the competent authorities.
- Recommendations/orders – following the review, the competent authorities will take the following actions:
  - (a) High risk determination:
    - (i) If the relevant authority determines that the CF poses a high risk of its being misused to disrupt the stable provision of the EIS, a recommendation is made for necessary measures to prevent actions disruptive to the EIS operator.
  - (b) An EIS operator's response:
    - (i) The EIS operator is required to make a notification within ten days from the receipt of the recommendation, indicating whether or not it will accept the proposed measures.
  - (c) Orders in the absence of response or rejection:
    - (i) If there is no notification regarding acceptance or rejection within the specified period, or if the EIS operator explicitly notifies that it does not accept the recommendation (unless there are legitimate grounds), the competent authority may proceed to issue orders for the implementation of the recommended measures.

This structured process would have a something of an influence on suppliers and vendors, since there is a possibility that they would not be able to carry out transactions with EIS operators due to the recommendation by the relevant authorities. Therefore, in practice they would be required to cooperate with EIS operators in order to effectively proceed with the screening process.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com