PANORAMIC

CYBERSECURITY

Japan

LEXOLOGY

Cybersecurity

Contributing Editors

Edward R McNicholas and Fran Faircloth

Ropes & Gray LLP

Generated on: July 19, 2024

Contents

Cybersecurity

Recent developments and future changes

Contributors

Japan

Nagashima Ohno & Tsunematsu

Yasushi Kudo yasushi_kudo@noandt.com
Tsubasa Watanabe tsubasa_watanabe@noandt.com
Hayato Maruta hayato_maruta@noandt.com

LEGAL FRAMEWORK

Key legislation

Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The Japanese government has enacted the Basic Act on Cybersecurity (BAC), which defines cybersecurity and mandates that both national and local governments formulate and implement cybersecurity policies. The BAC also establishes an obligation on private businesses and citizens to make efforts to ensure cybersecurity.

The Act on the Protection of Personal Information (APPI) also imposes on business operators handling personal information the obligation to take security measures to prevent leakage, loss or damage of personal data. These security control measures encompass technical, organisational, human and physical security control measures.

The Telecommunications Business Act (TBA) imposes on telecommunications carriers the obligation to establish rules for information handling, including security control measures to prevent incidents such as the leakage of users' information due to breach of communication confidentiality. These carriers must notify the Minister of Internal Affairs and Communications (MIC) of such rules.

These laws and other related laws and regulations ensure that businesses handling sensitive information adhere to stringent security standards to safeguard data integrity and confidentiality.

Law stated - 1 6 2024

Most affected economic sectors

Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The most affected are the following 15 sectors, as designated in Annex 1 of the Cybersecurity Policy for Critical Infrastructure Protection (CPCIP), developed by the Cybersecurity Strategy Center based on article 12 of the BAC.

- 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 Industry
- Port Transport.

The critical social infrastructure providers (CSIPs), as defined under article 3(1) of the BAC, doing business in these sectors are legally obliged to respond to a cybersecurity incident and report it to the competent regulatory authorities under business-related regulations established by the said authorities. The CSIPs are also obliged to make efforts 'to cooperate in the implementation of the cybersecurity policy that the national or local government implements' and ensure that they respond to the matters stipulated in the action plan established by the national government under article 6 of the BAC. Specifically, this efforts-basis obligation encompasses strengthening systems for incident response, developing safety standards, strengthening information sharing systems and employing risk management.

Law stated - 1 6 2024

International standards

Has your jurisdiction adopted any international standards related to cybersecurity?

Based on the Industrial Standardization Act, the Japanese government has established the Japanese Industrial Standards (JIS) as domestic standards for industry. The JIS refers to standards established by the International Organization for Standardization (ISO) as the international ideal. Therefore, the JIS related to information security also reflect the international standards related to information security established by the ISO. JIS that refer to the information security management system (ISMS) standardised by ISO include JIS Q 27000:2019, JIS Q 27001:2023, JIS Q 27002:2024, JIS Q 27006:2018, JIS Q 27014:2020 as a standard for governance of information security, and JIS Q 27017:2016 as a standard for security measures in response to cloud services.

Law stated - 1 6 2024

Personnel and director obligations

What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

The general interpretation in respect of directors' duty of care under the Companies Act is that it encompasses responsibility for managing cybersecurity risks through the establishment and operation of an internal control system. Therefore, directors, including representative directors and chief information security officers, are obligated to establish

and operate an appropriate cybersecurity system. Fulfilling this obligation entails managing and ensuring the adequacy of the organisation's cybersecurity defences.

In addition, in companies mandated to implement safety control measures and ensure the cybersecurity of their information based on the individual laws and guidelines, the person in charge of taking such measures and ensuring cybersecurity must evaluate and maintain the ISMS and overall cybersecurity system. This ensures ongoing compliance and the effectiveness of security measures.

Law stated - 1 6 2024

Key definitions

How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

Article 2 of the BAC defines cybersecurity as the state whereby measures are taken for appropriate security management, including the prevention of leakage, loss or damage of information recorded or communicated electronically, and for ensuring the safety and reliability of information systems and networks, and which state is properly maintained and managed. In Japan, data privacy and cybersecurity are treated as distinct concepts, and the APPI covers data privacy. However, the above definition encompasses measures for appropriate security control of information and the proper maintenance of these measures and overlaps with the obligation under the APPI to adopt security control measures for personal data. In addition, the National Police Agency, in Chapter 3 of its White Paper issued in 2024, defines cybercrime as 'violations of the Act on the Prohibition of Unauthorized Computer Access, crimes involving computer and electromagnetic records, and other crimes that use advanced information and communications networks as an essential means for their commission'.

Law stated - 1 6 2024

Mandatory minimum protective measures

What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

In Japan, while certain businesses are obligated to adopt safety control measures for cybersecurity pursuant to the relevant laws and regulations, there is no rigid definition of specific methods as minimum requirements; rather, these methods are presented as reference information in the applicable guidelines. Each business entity is evaluated based on its implementation of measures deemed equivalent to or higher than a certain level, ensuring security in consideration of the associated risks. For instance, the APPI outlines specific methods for implementing security control measures against cyber-attacks, and these methods are designed for business operators handling personal information. However, the methods are set forth as examples and their adoption is not compulsory.

In addition, entities designated as CSIPs under the BAC are mandated to implement certain safety control measures for cybersecurity. These measures are aligned with the laws governing their respective industries and are overseen by the relevant competent authorities.

Law stated - 1 6 2024

Cyberthreats to intellectual property

Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

In Japan, the Unfair Competition Act (UCA) serves as the legislation governing cyberthreats to intellectual property, imposing criminal penalties for various acts, including the acquisition of trade secrets through unauthorised access with the intent to gain an advantage for oneself or to infringe upon the advantage of a third party.

According to the UCA, a trade secret is defined as information meeting the following criteria:

- It must be kept confidential.
- It must consist of technical or business information that is beneficial for conducting business activities.
- It must not be publicly known.

Law stated - 1 6 2024

Cyberthreats to critical infrastructure

Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The BAC has identified 15 sectors encompassing critical infrastructure projects such as gas and electricity. Operators within these sectors are designated as CSIPs under the BAC. CSIPs are subject to, among other requirements, the CPCIP and its associated guidelines for establishing safety standards, as outlined in the BAC. Additionally, each CSIP is obligated to adhere to the cybersecurity regulations stipulated by the corresponding competent authority overseeing its sector. They are also required to collaborate with such agencies to bolster cybersecurity efforts.

Law stated - 1 6 2024

Restrictions on cyberthreat information sharing

Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Under the TBA in Japan, criminal penalties are prescribed for actions that violate the secrecy of communications. Consequently, there was debate regarding whether the sharing of cyberthreat information could potentially infringe upon this secrecy of communications.

In response to this issue, MIC, which supervises the telecommunications industry under the TBA, initiated a study group to address the matter. This study group has compiled a report that concludes that, to enable internet service providers to effectively

respond to cyberattacks, the sharing of specific information deemed necessary for cybersecurity measures by these providers does not constitute a violation of the secrecy of communications.

Law stated - 1 6 2024

Criminal activities

What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

The principal criminal cyber activities that are relevant to organisations are as follows:

- Unauthorised access to a computer system with restricted access via a network without legitimate authority, as provided in the Act on the Prohibition of Unauthorized Computer Access.
- Wrongfully creating electronic data used in processing a person's affairs, or using such data for illegitimate purposes, as provided in article 161-2 of the Penal Code.
- Creating or distributing malware without justifiable reason, as provided in article 168-2 and article 168-3 of the Penal Code.
- Interfering with a person's business by disrupting the operation of a computer used in the course of business, as provided in article 234-2 of the Penal Code. In addition, unjust economic gain by providing false information to a computer or by other means in relation to such a computer is punishable under article 246-2 of the Penal Code.

Law stated - 1 6 2024

Cloud computing

How has your jurisdiction addressed information security challenges associated with cloud computing?

To mitigate cybersecurity risks associated with the utilisation of cloud services, the Japanese government has implemented several measures. One of these measures is the establishment of JIS Q 27017:2016, which serves as the Japanese domestic standard for information security control measures specifically tailored for cloud services. This standard is based on the ISO framework. In addition, in response to these risks, the government has introduced the Information Security Management Assurance Program (ISMAP). ISMAP functions as a system to pre-evaluate and register cloud service providers that satisfy the security criteria set forth by the Japanese government. This initiative aims to provide assurance to users regarding the security posture of cloud service providers operating within Japan.

Law stated - 1 6 2024

Foreign organisations

How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Japanese cybersecurity-related laws are applied consistently, regardless of whether the business entity is domestic or foreign. Therefore, such laws apply equally to foreign businesses operating in Japan.

For instance, provisions in the APPI concerning the transfer of personal data to third parties and the international transfer of personal data are applicable to foreign businesses operating in Japan, especially if they transfer personal data to their overseas parent companies. Moreover, if a foreign parent company provides goods or services to individuals in Japan from outside the country and handles personal information in the process, the APPI's extraterritorial clause directly applies to this parent company, thereby subjecting it to the provisions of the APPI.

Law stated - 1 6 2024

BEST PRACTICE

Recommended additional protections
Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency, Japan (IPA) have published the Cyber Security Management Guidelines (CMG). These guidelines summarise '3 principles' that management needs to be aware of and '10 important items' that should be directed to the chief information security officer (CISO).

In addition, the competent authorities that supervise the operations of CSIPs have issued guidelines to the critical social infrastructure providers (CSIPs) they supervise, outlining safety control measures for cybersecurity initiatives.

Law stated - 1 6 2024

Government incentives
How does the government incentivise organisations to improve their cybersecurity?

The Japanese government has not implemented an incentive system to incentivise cybersecurity enhancements.

Law stated - 1 6 2024

Industry standards and codes of practice

Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The JIS in reference to the ISO has been established as the domestic standard in Japan.

Further, METI and Information-technology Promotion Agency, Japan (IPA) have published the CMG and a collection of practices for its implementation of the CMG for cybersecurity. The three principles and 10 directives set forth by the CMG are outlined below, respectively.

Three principles that management should be aware of:

- Principle 1: Management will promote measures under its own behest.
- Principle 2: Attention must be paid to cybersecurity measures throughout the supply chain.
- Principle 3: Proactive communication with stakeholders is necessary in both normal times and emergencies.
- Ten key cybersecurity management issues:
    - Directive 1: Recognise risks and develop an organisation-wide response policy.
    - Directive 2: Establish a risk management system.
    - Directive 3: Secure resources (budget, human resources, etc) for cybersecurity measures.
    - Directive 4: Identify risks and develop a plan in response to such risk.
    - Directive 5: Establish a mechanism to effectively respond to risks.
    - Directive 6: Continually improve cybersecurity measures through PDCA cycle.
    - Directive 7: Establish an emergency response system in the event of an incident.
    - Directive 8: Establish a business continuity and recovery system in preparation for harm caused by incidents.
    - Directive 9: Assess the status of the entire supply chain and take countermeasures.
    - Directive 10: Promote the collection, sharing and disclosure of cybersecurity information.

Law stated - 1 6 2024

Responding to breaches

Are there generally recommended best practices and procedures for responding to breaches?

The CMG developed and published by METI and IPA also contain reference materials for incident response.

Moreover, businesses handling personal data are required to implement safety management measures outlined in the Guidelines Regarding the Act on the Protection of Personal Information, formulated under the Act on the Protection of Personal Information (APPI). In

the event of a personal data breach, they must follow the procedures described in these guidelines.

Furthermore, the Japan Computer Emergency Response Team Coordination Center has issued an Incident Handling Manual to guide responses to incidents such as information leaks. Additionally, IPA has published a Security Incident Handling Manual specifically tailored for small and medium-sized enterprises.

For additional resources, the Japan Network Security Association, a non-profit organisation focusing on network security, maintains a list of security response providers and digital forensics companies that can offer assistance in the event of a cyber incident. This list serves as a valuable reference for businesses seeking support during such incidents.

Law stated - 1 6 2024

Voluntary information sharing

Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Currently in Japan, there is no legal framework that provides incentives for sharing information on cybersecurity incidents. However, the Basic Act on Cybersecurity (BAC) led to the establishment of the Cyber Security Council, aimed at facilitating the prompt sharing of information to enhance cybersecurity.

In 2023, the Cyber Security Council issued the Guidance for Sharing and Publicizing Information on Cyber Attacks, aiming to promote information sharing in the event of cyber-attacks. Moreover, in 2011, IPA initiated the Initiative for Cyber Security Information Sharing Partnership of Japan (J-CSIP) as a platform for information exchange and early response, primarily among manufacturers of critical infrastructure equipment.

Law stated - 1 6 2024

Public-private cooperation

How do the government and private sector cooperate to develop cybersecurity standards and procedures?

cybersecurity, the Japanese government convenes a conference body comprising government and private-sector experts. These bodies formulate, publish and enforce regulations based on the outcomes of their deliberations.

For instance, the CMG and the collection of practices, which aid in implementing the directives outlined in the CMG, are crafted and published by METI and IPA. These documents are developed with the input of private-sector experts who participate as members of the study committee, incorporating the results of their discussions.

Law stated - 1 6 2024

Insurance

Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

In Japan, numerous insurance companies provide cyber insurance policies.

Law stated - 1 6 2024

ENFORCEMENT

Regulatory authorities

Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which is formed as the secretariat of the Cybersecurity Strategy Headquarters under the Basic Act on Cybersecurity (BAC), is also tasked with formulating and operating the Cybersecurity Policy for Critical Infrastructure Protection (CPCIP).

The competent authorities that oversee the CPCIP's operations, such as the Japan Financial Services Agency, Minister of Internal Affairs and Communications (MIC), Ministry of Health, Labour, and Welfare, METI and the Ministry of Land, Infrastructure, Transport, and Tourism, are tasked with developing and implementing cybersecurity guidelines for the businesses under their supervision.

On the other hand, the National Police Agency and Public Prosecutor's Office possess criminal investigative authority over criminal acts, including cybercrimes. However, only the Public Prosecutor's Office has the authority to indict cybercrimes.

Law stated - 1 6 2024

Extent of authorities' powers

Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Under the BAC, NISC has the authority to request any person to provide materials, explanations, or other cooperation as necessary to carry out its duties. These duties include investigations to determine the causes of serious cybersecurity events and the evaluation of countermeasures. However, such requests are voluntary, and a person who refuses to cooperate will not face any adverse consequences.

In addition, under the Act on the Protection of Personal Information (APPI), the Personal Information Protection Commission (PPC) is empowered to request reports from business operators handling personal information, request submission of documents and conduct on-site inspections. These actions are taken when there are concerns regarding safety management measures, including cybersecurity, implemented by such business operators.

Furthermore, each government agency possesses extensive administrative supervisory authority over businesses within its jurisdiction. For instance, MIC oversees telecommunications carriers, while the Ministry of Health, Labour, and Welfare regulates pharmaceutical companies. Consequently, these administrative supervisory authorities may conduct investigations as needed, which may involve requesting reports and materials from businesses under their supervision, including matters related to cybersecurity.

Law stated - 1 6 2024

Most common enforcement issues

What are the most common enforcement issues and how have regulators and the private sector addressed them?

In recent years, unauthorised access and ransomware attacks have frequently resulted in the leakage of personal data and breaches of the secrecy of telecommunications. In response, PPC and MIC have taken administrative actions, such as requesting reports and materials and recommending business improvements, against businesses responsible for these breaches.

For example, in autumn 2023, there was unauthorised access to the internal systems of a well-known telecommunications carrier by way of a malware attack on an employee of a contractor to which the carrier had outsourced certain operations. This incident resulted in the leakage of a large amount of personal data. Consequently, PPC and MIC commenced administrative actions against the telecommunications carrier.

Law stated - 1 6 2024

Regulatory and data subject notification

What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

Under the APPI, if there is a breach of personal data (including leakage, loss or damage to personal data; hereinafter the same) or a threat thereof and there is a risk of harm to individuals' rights and interests associated with such data, the business operator handling the personal information is required to report the incident to PPC within approximately three to five days from identifying the incident and also to promptly notify the affected individuals. However, the PPC has delegated authority to the relevant authorities under the APPI, and such business operator must report to different parties depending on the type of business.

For example, banks and internet service providers are required to report personal data breaches to the Japan Financial Services Agency and MIC, respectively. Further, such business operators are generally required to report further details of the breach to the competent authorities within 30 days of learning about the personal data breach. In addition, under the Telecommunications Business Act (TBA), a telecommunications business carrier is required to 'promptly' report any incident of infringement of the secrecy of communications to the General Telecommunications Administration or the relevant

authority having jurisdiction over the location of its headquarters. The carrier must also report additional details within 30 days of learning about the incident.

Law stated - 1 6 2024

Penalties for non-compliance with cybersecurity regulations

What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

In addition to the criminal penalties for the cyber activities, violations of the safety control measures required under the APPI and other relevant laws and regulations such as the TBA may result in administrative penalties. These penalties can include business improvement orders against the violating business operator or the publication of the business operator's name by the relevant regulatory authorities.

Law stated - 1 6 2024

Penalties for failure to report threats and breaches

What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

If there is a breach of personal data or a threat thereof, and there is a risk of harm to individuals' rights and interests associated with such data, a prompt report to the PPC and other relevant authorities is required, followed by a detailed report within a specified period. Additionally, notification to the affected individuals is also mandated. If the business operator handling personal information fails to meet these obligations, the PPC may request a report or conduct an on-site inspection of the business operator.

As a result of this investigation, the PPC may issue administrative guidance, recommendations, or orders to the said business operator for improvement. If the said business operator makes a false report, refuses to report or fails to comply with the PPC's order, the business operator will be subject to criminal penalties.

If a telecommunications carrier fails to report a case or makes a false report in violation of the reporting obligation imposed on the said carrier when a case of infringement of the secrecy of communications occurs under the TBA, the telecommunications carrier will also be subject to criminal penalties.

Law stated - 1 6 2024

Private enforcement

How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

A lawsuit for damages may be possible based on tort law or for breach of contractual confidentiality obligations.

Law stated - 1 6 2024

THREAT DETECTION AND REPORTING

Internal policies and procedures

What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

The Personal Information Protection Commission (PPC) publishes security control measures that outline specific methods for business operators handling personal information, in accordance with the Act on the Protection of Personal Information (APPI) guidelines. However, these methods are provided as examples and are not mandatory. In Japan, certain business operators are required to implement safety control measures for cybersecurity pursuant to relevant laws and regulations. Nonetheless, there are no specific policies or procedures that organisations must put in place to comply with these safety control measures.

Law stated - 1 6 2024

Record-keeping requirements

Describe any rules requiring organisations to keep records of cyberthreats or attacks.

In Japan, there is no explicit legal requirement mandating the retention of records, including logs, documenting cyber threats and attacks. However, under the Basic Act on Cybersecurity (BAC), critical social infrastructure providers (CSIPs) are obligated to share information concerning cyber threats and attacks with competent authorities, in accordance with the Cybersecurity Policy for Critical Infrastructure Protection (CPCIP). Consequently, it is understood that CSIPs should maintain comprehensive records for a specified duration to facilitate the provision of such information and to address inquiries from competent authorities when deemed necessary.

Moreover, beyond entities covered by CSIPs, if a cyber-attack leads to or is anticipated to result in an imminent breach of personal data, reporting to the PPC becomes obligatory. In such instances, the retention of information related to cyber threats and attacks may be necessary to fulfil this reporting requirement adequately.

In addition, telecommunications service providers may be compelled by investigative agencies such as the National Police Agency, pursuant to the Act on Criminal Procedure, to maintain communication and other records pertaining to a specific individual or organisation for up to 60 days for criminal investigations. Consequently, it is customary for logs spanning this time frame not to be deleted.

Law stated - 1 6 2024

Regulatory reporting requirements

Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Both the APPI and the Telecommunications Business Act (TBA) mandate expeditious reporting to the PPC or other competent authorities in the event that a breach or potential breach of personal data or an occurrence of the infringement of the secrecy of the communication meet specific criteria. It is important to note that this reporting requirement is triggered solely by the occurrence of a breach or the presence of a threat of breach or such occurrence, without necessitating an actual breach. Additionally, there exists no legal obligation for a company to report to authorities when it has experienced an attack that has not yet resulted in a breach or threat of breach or such occurrence, nor is there a requirement to report vulnerabilities to authorities.

Furthermore, the mandated report must encompass various details, including a summary of the incident, the nature of the leaked or potentially leaked information, pertinent information regarding affected individuals and the root cause of the incident, among other relevant information.

Law stated - 1 6 2024

Time frames

What is the timeline for reporting to the authorities?

Under the regulations stipulated by the APPI, if a breach or a threat of breach of personal data occurs and there is a risk of harm to the rights and interests of individuals, business operators are obligated to expeditiously report the incident to PPC or other relevant supervisory bodies within approximately three to five days from the date of identifying the breach or potential threat. Further, they are generally required to provide an additional detailed follow-up report within 30 days of the initial identification date.

Under the TBA, a telecommunications carrier is required to 'promptly' report any incident of infringement of the secrecy of communications to the competent authority having jurisdiction over the location of its headquarters. The carrier must also report additional details within 30 days of learning about the incident.

Law stated - 1 6 2024

Other reporting requirements

Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

CSIPs defined under the BAC necessitate the dissemination of cyber threat intelligence and information on cyber-attacks to competent authorities, aligning with the guidelines set forth by the CPCIP.

Moreover, the APPI imposes distinct notification responsibilities on business operators handling personal data. Should there be a breach or a threat of breach of personal data meeting specific criteria, these operators are obligated to notify the individuals associated with said data.

Listed companies, as mandated by the Financial Instruments and Exchange Act, must disclose annual financial statements and related documents. These statements necessitate the comprehensive delineation of business risks, encompassing cybersecurity threats among them. Consequently, there has been a discernible uptick in the disclosure of cybersecurity risks by an expanding cohort of listed companies in recent years.

In cases of cybersecurity breaches such as information leaks, listed companies may find themselves obligated to promptly disclose the incident and their response measures, subject to meeting specific criteria outlined in the timely disclosure regulations established by each securities exchange. However, even if these criteria are not met, a listed company reserves the option to voluntarily disclose the security breach in a timely fashion.

Law stated - 1 6 2024

UPDATE AND TRENDS

Recent developments and future changes

What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

The Information-technology Promotion Agency, Japan publicly reported '10 Major Security Threats 2024', which concerns threats to enterprises, attacks exploiting vulnerabilities embedded in the supply chain are ranked as the second-highest threat, while damage caused by ransomware attacks is ranked first.

Therefore, in Japan, in addition to ransomware attacks, dealing with supply chain risks has become a challenging risk in cybersecurity.

In light of supply chain vulnerabilities, Japanese corporations are significantly emphasising the necessity of addressing supply chain risks within their operational frameworks. They are turning to a range of guidelines provided by organisations such as the Cybersecurity Management Guideline and Cybersecurity Policy for Critical Infrastructure Protection (CPCIP) to inform their risk response strategies. Collaborative initiatives with business associates are deemed indispensable in effectively mitigating these risks.

Given this trend, the Japanese government has established a system (System) operational from May 2024, under the Economic Security Promotion Act to ensure provision of essential infrastructure services (EIS) and enhance the supply chain risk management, including ensuring cybersecurity in the EIS. The System is aimed at fortifying EIS resilience against cyber threats and ensuring a comprehensive response to emerging challenges. Under the System, (1) EIS encompasses services in electricity, gas, oil, water, railways, truck transport, international maritime cargo, aviation, airports, telecommunications, broadcasting, postal services, financial services, credit cards and port transport and (2) competent authorities of the Japanese government conduct a prior screening process and issue recommendations or orders concerning the installation or entrustment of maintenance, etc, of the critical facilities of EIS.

In response to the screening process under the System, it is likely that the suppliers and vendors of EIS operators would not be able to carry out transactions with EIS operators as a result of the recommendation by the relevant authorities. Therefore, the System is likely to incentivise and promote collaborative work between EIS operators and the suppliers and vendors of EIS operators to enhance the cybersecurity resilience in the supply chain risk management.

Law stated - 1 6 2024