Information Management

GRI 103-2

Why

— Why it matters —

Even as the development of IoT creates new value, cyberattacks are growing increasingly sophisticated and widening in focus from traditional IT to encompass the IoT/OT field as well. The risks for corporations include leaks of information, operational stoppages, and even direct disruption to business making information security one of the most critical issues companies face. Hitachi, in developing its Social Innovation Business, has highlighted the vital importance of information security governance as a key management issue and is working to address it.

With the arrival of the digital age due to advances in IT and the globalization of socioeconomic activity, privacy risks have also increased. Data associated with individuals, including location information and purchase history, has come to be known collectively as "personal data." The use of personal data can be expected to create value going forward, but protecting this data and showing due consideration for privacy is essential.

Information Security

What

— What we are doing —

- Disseminating information security policies
- Strengthening information management
- Preventing information leaks
- Providing education programs on information security
- Conducting thorough information security audits and inspections
- Personal information protection
- Managing customer information

How

— How we are doing it —

Policy and promotion structure

Hitachi has established Information Security Policies that foster cybersecurity risk management. The Information Security Committee is chaired by the chief information security officer (CISO) who has the responsibility and authority for the implementation and operation of Hitachi's information security and personal information protection systems. The committee determines relevant policies and measures, while the information security heads at each Hitachi business unit (BU) and Group company promote workplace awareness and oversee measure implementation.

	Achievements in Fiscal 2020
Strengthen information management	In addition to ISO/IEC27001, which is an international standard, we are promoting compliance with the U.S. government standard SP800-171 in our Global Information Security Management Regulations to strengthen information security governance globally. Built a cyber monitoring environment that continually adopts the latest technology to defend against increasingly sophisticated cyberattacks
Provide education programs on information security	Held e-learning programs on information security and personal information protection (participating employees: around 40,000)
Conduct thorough information security audits and inspections	Conducted Information security and personal information protection audits at all Group companies and business units (annual) Conducted audits of 153 Hitachi Group companies in Japan including Hitachi, Ltd. in the same manner as at Hitachi, Ltd. and Hitachi, Ltd. confirmed all results
Personal information leaks	Personal information leaks: 0
Privacy protection initiatives by Hitachi's IT Sector	· Published opinion surveys on use of consumer data in big data businesses · Hitachi initiatives were included in the *Guidebook on Corporate Governance for Privacy in Digital Transformation (DX) ver.1.1* released by Japan's Ministry of Internal Affairs and Communications and Ministry of Economy, Trade, and Industry.

Information Security

Information Security Policies

Policy

Hitachi considers one of its top management priorities to be information security governance to minimize the risk of business disruption such as leaks of information or operational stoppages due to cyberattacks. The Japan Business Federation's Declaration of Cyber Security Management also places emphasis on cyber security measures as a critical management challenge from the aspects of both value creation and risk management. Hitachi approaches the issue of information security governance based on the same philosophy.

At the same time, as a global company, we regard cyber security risk as one of our management risks. Accordingly, to enable us to declare both internally and externally Group policies for addressing this risk, we have formulated Information Security Policies in line with our corporate management policies and based on our cyber security risk management.

We have our data centers and other divisions certified by the ISMS Accreditation Center in accordance with the ISO/IEC 27001 Information Security Management System international standard. This certification has been received by seven divisions of Hitachi, Ltd. and 28 divisions of 23 Group companies.[*1]

[*1] As of March 31, 2021.

Information Security Policies

1. Formulation and continuous improvement of information security management regulations
2. Protection and continuous management of information assets
3. Strict observance of laws and standards
4. Education and training
5. Incident prevention and management
6. Assurance of fair business practices within the corporate group

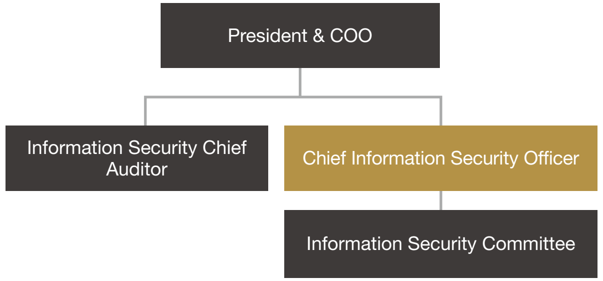
Framework for Promoting Information Security

Structure

At Hitachi, Ltd., the Chief Information Security Officer (CISO), who is the C-level executive with ultimate authority and responsibility regarding the handling of information security and personal privacy issues oversees the promotion of information security for all Hitachi products, services, and internal facilities.

Chaired by the CISO, the Information Security Committee determines all policies and procedures for information security and personal information protection. As a general principle, heads of business units and divisions serve as information security officers. They also establish information security promotion departments, work to implement information security management in each workplace, and provide relevant education to employees. This framework is also implemented at Group companies to promote information security across the Group through mutual cooperation.

Framework for Promoting Information Security


President & COO
Information Security Chief Auditor
Chief Information Security Officer
Information Security Committee

Information Security Management

Structure

Hitachi establishes its Global Information Security Administration Rules which conform to the international ISO/IEC 27001 standard and follows NIST Special Publication 800-171 (National Institute of Standards and Technology of the Department of Commerce in the United States) to reinforce its information security. These rules are globally distributed by the headquarters of Hitachi, Ltd. and its Group companies. Other measures include actively promoting the use of shared security services and related support for information security provided by regional headquarters in the Americas, Europe, Southeast Asia, China, and India.

The Information Security Promotion Council and other bodies convey policies and procedures for information security and personal information protection determined by the Information Security Committee internally and to other companies in the Hitachi Group. Information security officers at business sites and companies ensure that these decisions are implemented in the workplace.

Details of our information security initiatives are contained in our Information Security Report.

Information Security Report

Achievements in and after Fiscal 2020

As Hitachi promotes new workstyles based on telecommuting, the vulnerability posed by employees' security awareness becomes a risk. Given this threat, we are working to raise security awareness among our employees with an employee-centered approach alongside IT-based security measures.

Security Monitoring

In Hitachi, the Security Operation Center (SOC) monitors security on a round-the-clock basis so global-scale cyberattacks can be detected and countermeasures initiated right away. The Incident Response Team (IRT) collects and develops threat intelligence[*1] and manages the response to any security incidents.

Every year, cyberattacks become more sophisticated with damage tending to increase as attacks slip past conventional detection and go undiscovered for longer periods. To counter this risk, in fiscal 2020 we began building a cyber monitoring environment that always uses the latest technology.

[*1] Threat intelligence: An approach to countering cyberattacks using knowledge of new threats gathered from multiple sources of information on cyber security.

Preventing Information Leaks

Structure

Hitachi takes the following IT steps to prevent information leaks: encrypting devices; using thin clients;[*1] employing electronic document access control and expiration processing software; maintaining ID management and access control by building an authentication infrastructure; and filtering e-mails and websites. In response to the recent spate of targeted e-mail attacks and other cyberattacks, we are participating in an initiative to share information between the private sector and the government. We are also enhancing various IT measures such as a defense in depth strategy.

To prevent leaks from our suppliers, we review their information security measures based on Hitachi's own standards before allowing them access to confidential information. We also provide tools to suppliers for security education and for checking business information on computers. In addition, we require suppliers to check and remove business information from personal computers.

[*1] Thin client: A terminal with the minimum necessary software. Thin client computing significantly enhances cyber security by storing applications and data on the server.

Education on Information Security

Employee Engagement

Hitachi holds annual e-learning programs on information security and personal information protection for all executive officers and employees. More than 40,000 employees at Hitachi, Ltd. participate in these programs, and the participation rate has reached almost 100%. We offer a variety of courses that have different goals and are tailored to different target audiences, including new employees, new managers, and information system administrators. We also implement simulation training to educate employees about phishing attacks and other cyberattacks. Employees are sent deceptive e-mails as phishing simulations to heighten their awareness of security through direct experiences.

Educational programs from Hitachi, Ltd. shared within the Group provide Group-wide education on information security and personal information protection.

Thorough Information Security Audits and Inspections

Activities

The Hitachi Group has developed its approach to security based on the "Plan-Do-Check-Act" (PDCA) cycle for its information security management system. We conduct annual information security and personal information protection audits at all Group companies and business units.

The president of Hitachi, Ltd. appoints officers to conduct independent audits. These officers are not allowed to audit their own units, underlining our commitment to fairness and objectivity in auditing.

There are 153 Hitachi Group companies in Japan, including Hitachi, Ltd., that conduct audits in the same way as Hitachi, Ltd., and all results are subject to confirmation. For Hitachi Group companies outside Japan, we use a common global self-check approach to ensure Group-wide auditing and inspections. All business units conduct Confirmation of Personal Information Protection and Information Security Management annually as self inspections. We conduct monthly Confirmation of Personal Information Protection Management at 733 operations (as of March 2021) that handle important personal information. This regular control mechanism ensures ample safety management and implementation.

Personal Information Protection

Personal Information Protection Policy

Structure

Hitachi, Ltd.'s Personal Information Protection Policy sets out its corporate philosophy and principles on personal information protection. The policy is disseminated to all executive officers and employees as well as being publicly available.

A personal information protection management system based on the policy has also been established. Through the rollout of the system, as well as the safe handling of personal information, programs for all employees, and periodic audits we are ensuring protection of personal information.

Personal Information Protection Policy

PrivacyMark[*1] Certification

Activities GRI 418-1

Hitachi, Ltd. has received PrivacyMark certification. The entire Hitachi Group is committed to personal information protection with 39 Hitachi Group companies having received the PrivacyMark as of March 31, 2021.

Hitachi also strives to safeguard personal information globally at Group companies outside Japan based on each company's personal information protection policy and ensures that they comply with all applicable laws and regulations in each country and region as well as the expectations of society at large.

There were no cases of personal information leakage during fiscal 2020.

[*1] PrivacyMark: A third-party certification established in April 1998 that is granted by the assessment body the Japan Information Processing Development Corporation to businesses that have taken appropriate security management and protection measures related to personal information.

Responding to Personal Data Protection Laws Around the World

System

With the increasing risk of privacy violations in recent years due to the advent of the digital age following advances in IT and the globalization of socio-economic activities, lawmakers are actively seeking to create and modify relevant laws and legislation in countries and regions around the world. Hitachi pays close attention to relevant laws and legislation on a global basis including the European General Data Protection Regulation (GDPR) and makes efforts to comply with them across the Group. We also monitor relevant legislation and social trends and take action when necessary.

Management Framework for Customer Information

Structure

Hitachi has deployed customer relations management (CRM) systems at approximately 200 Group companies, which allow us to collect and accurately manage customer and transaction information, in addition to using it as a marketing tool. This covers more than 80% of the orders received across the whole Group with the database enabling us to formulate more effective sales strategies and offer collaborative solutions by multiple businesses.

Privacy Protection Initiatives by Hitachi's IT Sector

Approach Activities

We are taking proactive steps to protect privacy to ensure that personal data is used safely and securely. In our IT sector, which leads our digital business, we have assigned a personal data manager responsible for privacy protection and established a privacy protection advisory committee to support risk assessments and develop countermeasures based on its knowledge and expertise of privacy protection. In accordance with the policies set by the committee, our employees implement privacy impact assessments for processes where personal data will be handled and take measures to prevent privacy violations. In fiscal 2020, the number of cases where personal data was handled increased because of our measures against COVID-19. The committee has issued guidance on privacy protection items of this sort and is putting measures in place based on this guidance.

Furthermore, we regularly conduct consumer opinion surveys on the use of consumer data in big data businesses. The 2020 survey revealed trends thought to be attributable to the current social climate such as expectations for measures using personal data to help counter the spread of COVID-19. Initiatives to regularly survey consumer opinions and then use this information to assess and improve measures are regarded as important and are taken up as examples in the *Guidebook on Corporate Governance for Privacy in Digital Transformation (DX) ver.1.1* published by Japan's Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade, and Industry.