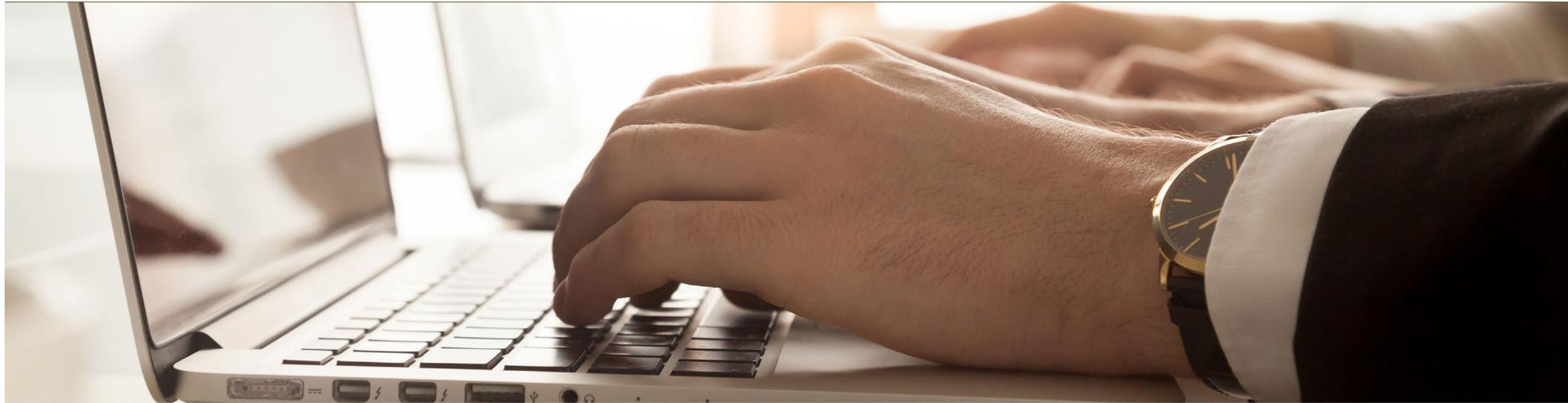


Information Management



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. The development of Hitachi's Social Innovation Business has highlighted the vital importance of information security governance as a key management issue, and measures are being put in place to address it.

With the arrival of the digital age due to advances in IT and the internationalization 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. Hitachi not only implements comprehensive personal information management, strictly adhering to all relevant laws and regulations in every country and region where it does business, it also aims to create value by using personal data safely and securely while keeping privacy protected.

What we are doing

	Core initiatives	Goals and KPIs	Achievements in FY 2019
 <p>Information security</p>	<ul style="list-style-type: none"> Disseminate Information Security Policies Strengthen information management Prevent information leaks Provide education programs on information security Conduct thorough information security audits and inspections 	<ul style="list-style-type: none"> Information security and personal information protection audits at all Group companies and business units (annual) 	<ul style="list-style-type: none"> Launched cyber security risk-management activities

What we are doing

	Core initiatives	Goals and KPIs	Achievements in FY 2019
 <p>Personal information protection</p>	<ul style="list-style-type: none"> • Protect personal information • Manage customer information • Manage online content 	<ul style="list-style-type: none"> • Personal information leaks: 0 	<ul style="list-style-type: none"> • Held e-learning programs on information security and personal information protection (participating employees: around 40,000) • Conducted opinion surveys on use of consumer data in big data businesses • Developed e-learning tool on using social media and addressing associated risks

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 placed 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 concept.

At the same time, as a global company, we regard cyber security risk as one of our management risks. Accordingly, to allow 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 ISMS-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 7 divisions of Hitachi, Ltd. and 27 divisions of 21 Group companies.*1

*1 As of July 31, 2020.

Information Security Policies

1. Formulation and continuous improvement to 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

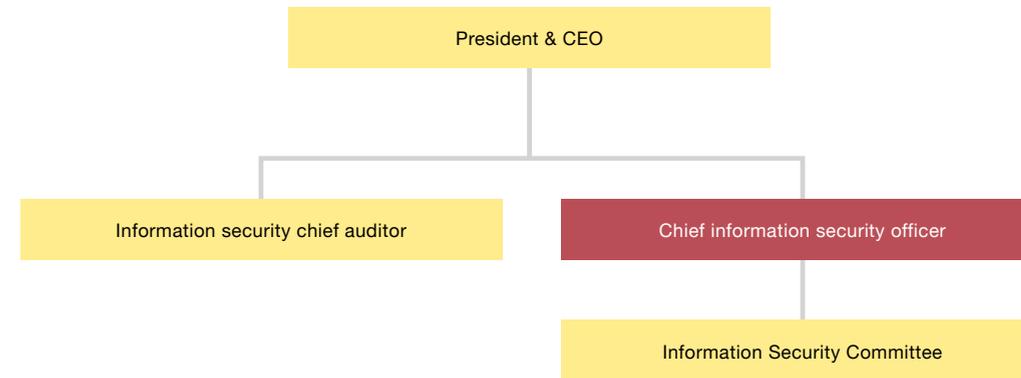
Framework for Promoting Information Security

Structure

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

Chaired by the CISO, the Information Security Committee determines all policies and procedures for information security and personal information protection. These decisions are conveyed to all Hitachi Group business sites and companies, and are implemented by the relevant information security officers.

■ Framework for Promoting Information Security



Information Security Management

Structure

Hitachi reinforces its information security in line with its Global Information Security Administration Rules, which conform to the international ISO/IEC 27001 standard. 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 Committee determines policies and procedures for information security and personal information protection. The Information Security Promotion Council and other bodies convey decisions 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 2018 (latest edition) ▶
https://www.hitachi.com/sustainability/download/pdf/securityreport_e.pdf

Achievements in FY 2019

As cyberattack methods become more diversified, our business is at a higher risk of damage from incidents taking place in a broader range of areas. To address this risk, in fiscal 2019 we expanded the scope of our risk management from the security of the internal IT environment used by our existing OA to launch a new series of cyber security risk management activities. We are currently working to reduce business risk by expanding our efforts in the environments where products and services are developed, produced, and manufactured as well as the supply chain and the process of developing products and services.

Security Monitoring

In Hitachi, the Security Operation Center (SOC) monitors security on a 24/7 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.

*1 Threat intelligence: An approach to countering cyberattacks using knowledge of new threats gathered from a range 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-mail and visited 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 our IT organization by adding more layers to our leak prevention procedures.

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 (procurement partners) 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.

Nearly all of the roughly 40,000 employees at Hitachi, Ltd. participate in these programs. 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 malicious targeted e-mail attacks and other cyberattacks. Employees are sent examples of targeted e-mail to heighten their awareness of security through direct experience.

Our educational programs, 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 196  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. We implement Confirmation of Personal Information Protection and Information Security Management annually for the voluntary inspection of Hitachi, Ltd. business unit workplaces. We conduct monthly Confirmation of Personal Information Protection and Information Security Management assessments at 629 operations (as of March 2020) that handle important personal information. This regular control mechanism ensures ample safety management and implementation.

Personal Information Protection

Personal Information Protection Policy

Policy

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.

Privacy Mark*1 Certification

Activities

418-1

Hitachi, Ltd. received Privacy Mark certification. The entire Hitachi Group is committed to personal information protection, with 39 Hitachi Group companies having received the Privacy Mark as of March 31, 2020.

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

There were no cases of personal information leakage during fiscal 2019.

*1 Privacy Mark: A third-party certification established in April 1998 that is granted by the assessment body 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 violation 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. The Hitachi Group pays close attention to relevant laws and legislation on a global basis, including the European General Data Protection Regulation (GDPR), making efforts to comply with them across the Group. It also monitors relevant legislation and social trends and takes action in response when necessary.

Management Framework for Customer Information

Structure

Hitachi's customer relations management framework, HiCRM, has been deployed at approximately 200 Group companies to collect and accurately manage customer and transaction information Group-wide, in addition to serving as a marketing tool. HiCRM 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. Going forward, we will consider rolling out the system more aggressively across the Group.

Privacy Protection Initiatives by Hitachi's IT Sector

Approach & Activities

We are taking proactive steps on privacy protections to ensure that personal data is used safely and securely.

In Hitachi's IT sector, which leads our digital business, we have assigned a personal data manager responsible for managing privacy protection and established a privacy protection advisory committee to support risk assessments and develop countermeasures based on 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. When employees find it difficult to assess risks on their own, or conclude that risks of privacy violation are high, the privacy protection advisory committee will extend support to deal with the case and help reduce risks. In fiscal 2019, we dealt with 190 privacy protection cases of this sort.

In order to leverage the expertise built on these experiences when conducting business with our customers, we have made publicly available a whitepaper on Hitachi's privacy protection initiatives in the use of personal data. Furthermore, Hitachi regularly conducts consumer opinion surveys on the use of consumer data in big data businesses to understand changing consumer perceptions and take them into consideration when updating privacy protection measures.



Hitachi Personal Information Protection Policy
<http://www.hitachi.com/privacy-e/>

Online Content Management

Information Management Policies on the Use of the Web and Social Media

[Policy](#)

Hitachi has been active in promoting initiatives to deepen customer understanding of its Social Innovation Business through its corporate website and social media accounts. To protect our brand and avoid violating the rights of others, including human rights, in implementing these initiatives, we have established the Hitachi Social Media Policy for global use, which stipulates usage policies. To raise awareness of this policy, an e-learning tool on approaching the use of social media and addressing associated risks is available in Japanese, English, and Chinese.