Advancing Risk Management on Multiple Fronts

Hitachi's Approach

Changes to our operating environment from such factors as the globalization of the economy and advances in and spread of information and communications technology (ICT) lead not only to the expansion of business opportunities but also to the diversification of risks to our operations.

We have built a diverse risk management system under which we carry out risk analysis to accurately gauge ongoing economic and social changes and use the insights gained to take preventive measures and ensure a rapid response to issues that may arise unexpectedly.

Particularly in recent years, as a company deeply involved in infrastructure projects in countries and regions around the world, we take note of the discussions at meetings like the World Economic Forum on such international risks as the unending series of terrorist attacks, the increasing severity of abnormal weather conditions, global-scale climate change, and the growing scale and sophistication of cyberattacks.

We are reinforcing business continuity plans (BCPs) and further tightening our information security to ensure the stable supply of our products and services and to prevent threats to our networks that could severely disrupt business operations. We will continue to reinforce our risk management on a Group-wide basis and make thoroughgoing efforts to minimize risks to society from our operations.

Risk Management

Reinforcement of Risk Management System

The entire Hitachi Group is reinforcing its risk management system to address increasingly globalized and complex risks.

Under Hitachi, Ltd.'s head of risk management, each business operation assigns an executive as its risk management officer to manage risks mainly concerned with compliance, export control, disasters, and crime, and to respond adequately in coordination among the entire Group. Furthermore, Hitachi is building a comprehensive risk management system that contains standards and procedures to objectively evaluate different risks that may affect business.

Stable Provision of Products and Services

Creating BCPs in Key Operations Worldwide

Given the close relation of our business to social infrastructure, we are enhancing our business continuity plans (BCPs) to ensure that the impact of risks does not disrupt our business and thereby significantly affect society. In December 2006, we issued the *Hitachi Group Guidelines for Developing Business Continuity Plans (Overview)* in Japanese. In fiscal 2010 this was translated into English and Chinese for distribution to all Hitachi Group companies worldwide to ensure our response readiness for large disasters and other risks.

When the Great East Japan Earthquake struck in March 2011, our BCPs enabled quick responses and swift decision making. However, issues emerged, including identification of

secondary and other suppliers, cloud storage and multiplexing of production information, and the need to secure alternate transportation and fuel sources. Based on the lessons learned from this disaster, in October 2011 we released and distributed new versions of the *Hitachi Group Guidelines for Developing Business Continuity Plans* for individual departments to further improve our BCPs.

By the end of fiscal 2011, Hitachi Group operations in Japan had completed their preparation and review of BCPs for both large earthquakes and novel strains of influenza as appropriate to their operations.

On top of these efforts, Hitachi, Ltd. has held annual earthquake drills simulating a major seismic event at key operations in Japan since fiscal 1998. In March 2017, Hitachi Chemical held drills under the direction of its head office general manager, with managers at the head office and the Nabari Works striving to improve their risk management skills and identify possible areas for improvement in their BCPs.

Hitachi appointed personnel with responsibility for risk-response policies at its main overseas bases in fiscal 2013. By the end of that year, around 300 companies had prepared BCPs with the goal of completing them for key operations. These BCPs are aimed at strengthening our ability to respond to business risks, including large disasters, novel strains of influenza, political instability, and social disruption, as well as acts of terrorism. Moving forward, we intend to further expand the scope of our BCPs.
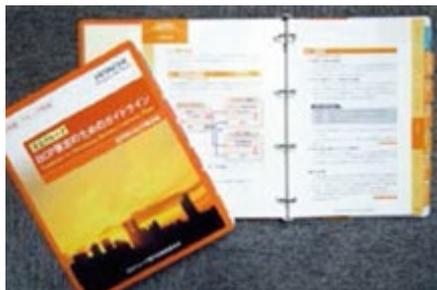
Hitachi Group Guidelines for Developing Business Continuity Plans (for individual departments).

Earthquake simulation drill.

Creation of Procurement BCPs

We have a deep involvement in social infrastructures in places where the suppliers who are our business partners can be affected by major earthquakes and other natural disasters.

These disasters can heavily impact not only our business operations and those of our suppliers but also society as a whole. To minimize this impact, the procurement divisions in business units and key Group companies in Japan have created procurement BCPs that (1) standardize and use generic parts to make procurement as flexible as possible; (2) cultivate multiple suppliers; (3) distribute production across several locations; (4) budget inventory strategically; and (5) consider

substitute products. To see whether or not procurement BCPs would be effective, we held desktop exercises to discuss in a group what should be done during and after a disaster, making further improvements as a result.

In fiscal 2016, all major Group business sites with production lines (approximately 200 sites in total) took steps to maintain and strengthen the procurement BCPs they had created by the previous fiscal year, thereby contributing to the continuation of Hitachi's global operations.

Improving Safety for Employees Sent to Dangerous Regions

Responding to the hostage incident in Algeria in January 2013, then President Hiroaki Nakanishi reinforced his policy in February 2013 of ensuring the safety of employees sent to countries and areas at higher risk. Survey missions of in-house and outside experts are now sent beforehand to areas at high risk of war, terrorism, and other threats. Even after employees are dispatched to such areas, we conduct additional local surveys every six months as a means of confirming the effectiveness of our safety policies. In fiscal 2016, with the threat of terrorism expanding around the world, we introduced a range of safety measures, including providing timely alerts to employees. This underscores our commitment to ensuring the safety of our employees working around the globe. Hitachi is also contributing to safety measures at other Japanese corporations operating outside Japan. To help enhance collaboration between the private and public sectors in this area, Hitachi executives participated in the Council for Public-Private Cooperation for Overseas Safety organized by Japan's Ministry of Foreign Affairs. Since 2014 Hitachi, Ltd. has taken part in public-private kidnap incident preparatory training exercises.

Promoting Information Security

Implementing Rigorous Information Security

Hitachi's chief information officer (CIO) is appointed by the company's president and has the authority and responsibility to implement and operate an Information Security Management System (ISMS). In fiscal 2016, the role of the CIO was performed by Hitachi's senior vice president and executive officer. The Information Security Committee, chaired by the CIO, 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.
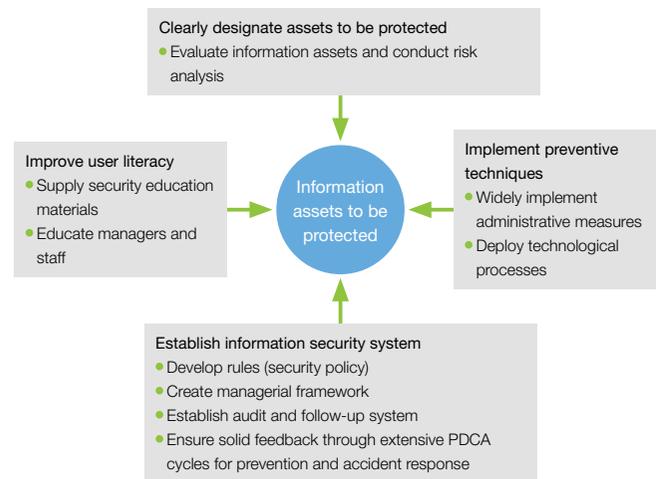
The Hitachi Group emphasizes two points in information security and personal information protection:

(1) Precautionary measures and prompt security responses
   We classify assets to be secured and take safeguarding measures based on vulnerability and risk analyses. We also have an emergency manual for security breaches, based on the assumption that these are inevitable, and not just possible.
(2) Promoting stronger ethical and security awareness among data users
   We have prepared a program tailored to Hitachi's various personnel levels and are working to raise the prevailing sense of ethics and security awareness through Group-wide e-learning. We are also conducting audits to identify and address problems early on.

Details, including a message from the CIO and a list of third-party assessments and certifications, are contained in *Information Security Report 2016*.

🖱 *Information Security Report 2016*

Basic Approach to Information Security Governance

Clearly designate assets to be protected
- Evaluate information assets and conduct risk analysis

Improve user literacy
- Supply security education materials
- Educate managers and staff

Information assets to be protected

Implement preventive techniques
- Widely implement administrative measures
- Deploy technological processes

Establish information security system
- Develop rules (security policy)
- Create managerial framework
- Establish audit and follow-up system
- Ensure solid feedback through extensive PDCA cycles for prevention and accident response

Education on Information Security

Consistently maintaining information security requires all parties to continually develop their knowledge of information handling and to remain strongly aware of the issues. For this reason, we hold annual e-learning programs on information security and personal information protection for all directors, employees, and temporary 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. In 2012, we also began simulation training to educate employees about the increasing trend toward 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, available to Hitachi Group companies in Japan and other global regions, provide Group-wide education on information security and personal information protection.

Preventing Information Leaks

Hitachi, Ltd. has formulated the Three Principles for Preventing Leakage of Confidential Information to ensure the highest level of care for such information and to prevent leaks and other related incidents. Our policies ensure that if an incident does occur, damage is promptly minimized by contacting customers, reporting to government agencies, investigating causes, and acting to prevent any recurrence.

We take the following IT steps to prevent information leaks: using encryption software and secure PCs; 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, including both entry and exit countermeasures.

To ensure the secure exchange of information with our suppliers, we review their information security measures based on Hitachi's own standards before allowing them access to confidential information. We have provided 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 to prevent leaks.

In the May 2017 global cyberattack, ransomware that functions like a network worm affected parts of Hitachi's in-house system, temporarily disabling the sending and receipt of e-mails. No information leaks were detected, however, and there was no damage to customers or other outside parties through e-mail sent from the Hitachi Group.

🖱 Damage Caused by Ransomware, and Status of Recovery

Three Principles for Preventing Leakage of Confidential Information

Principle 1

As a general principle nobody can take Confidential Information out of the Company's premises.

Principle 2

Any person taking Confidential Information out of the Company's premises due to business necessity shall obtain prior approval from the Information Assets Manager.

Principle 3

Any person taking Confidential Information out of the Company's premises due to business necessity shall put in place relevant and appropriate measures against information leakage.

Global Information Security Management

Hitachi Group companies worldwide reinforce their information security in line with our Global Information Security Administration Rules, which conform to the international ISO/IEC 27001 standard. These rules are distributed from the parent company in Japan to Group companies around the world. Other security measures include secure shared services and support from our regional headquarters in the Americas, Europe, Southeast Asia, China, and India.

Thorough Information Security Audits and Inspections ✓

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 222 Hitachi Group companies in Japan 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 business unit workplaces. We conduct monthly Confirmation of Personal Information Protection and Information Security Management assessments at 654 operations (as of March 2017) that handle important personal information. This regular control mechanism ensures ample safety management and implementation.