Risk Management

Advancing Risk Management on Multiple Fronts

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.

Reinforcement of Risk Management System

The entire Hitachi Group is reinforcing its risk management system to address increasingly globalized and complex risks. Under the head of risk management at Hitachi, Ltd., 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.

Risk Factors

We conduct business on a global scale across a broad range of business areas and utilize sophisticated, specialized technologies to carry out our operations. Therefore, we are exposed to risks attributable to the economic environment, risks inherent in individual industrial sectors and business lines, and risks related to our operations. Investment in our securities also involves risks. The following risks are based on the assumptions we consider reasonable as of the date this report was issued.

- Economic Trends
- Currency Exchange Rates Fluctuations
- Access to Liquidity and Long-term Financing
- Marketable Securities Risks
- Material and Component Procurement
- Estimates, Fluctuations in Cost and Cancellation of Long-term Contracts
- Credit Risks Arising from Business Transactions
- Supply and Demand Balance
- Rapid Technological Innovation
- Dependence on Specially Skilled Personnel
- Intense Competition
- Our Strategy to Strengthen Our Social Innovation Business
- Acquisitions, Joint Ventures, and Strategic Alliances
- Restructuring of Our Business
- Worsening of Business Performance of Equity-method Associates and Joint Ventures,
- Our Overseas Growth Strategies
- Overhaul of Cost Structure
- Intellectual Property
- Litigation and Regulatory Investigations
- Product Quality and Liability
- Significant Disasters and Similar Events
- Dependence on Information Systems
- Management of Confidential Information
- Employee Retirement Benefits
- Dilution of Your Shares by Issuances of Additional Shares

Please refer to the Company's annual securities report for the fiscal year ended March 31, 2018 for details of business and other risks.
http://www.hitachi.com/IR-e/library/stock/index.html

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 2018, we held initial response drills at our headquarters under the direction of our head office general manager simulating a large earthquake in the Tokyo area, striving to promote understanding of each department's role and strengthen cooperation among departments.

As part of countermeasures against large earthquakes striking the Tokyo metropolitan area, in December 2017 we developed action plans including setting up substitute headquarters in the Kansai region in case our Tokyo headquarters cease to function temporarily due to such earthquakes.

Hitachi appointed personnel with responsibility for risk-response policies at its main overseas bases in fiscal 2013. By the end of that year, approximately 300 companies 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.

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 2017, all major Group business sites with production lines (approximately 208 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 2017, with the threat of terrorism expanding around the world and infectious diseases spreading regionally, 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 has taken part in public-private kidnap incident preparatory training exercises.

Promoting Information Security

Information Security Policies

The increased connections between things due to development of IoT are creating new value. At the same time, increasingly creative cyberattacks are widening their focus from traditional IT to include the IoT/OT field. Managing information security risks is one of the most critical issues for companies to minimize the risk of business disruption due to factors such as leaks of information or operational stoppages.

The development of the Social Innovation Business has highlighted for Hitachi the vital importance of information security governance as a key management issue. The Japan Business Federation's Declaration of Cyber Security Management that was published in March 2018 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.

Information Security Set-up

At Hitachi, Ltd. the senior executive with ultimate authority and responsibility regarding the handling of information security and personal privacy issues is appointed by the President & CEO. Previously, the CIO[*1] oversaw information security.

In October 2017, in a move aimed at upgrading the governance of information security for the Group and to centralize the promotion of related measures, Hitachi established a new position of CISO[*2] to oversee promotion of information security for all Hitachi products and internal facilities. In fiscal 2017, the CISO role was performed by an executive vice president.

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.

[*1] CIO: Chief Information Officer
[*2] CISO: Chief Information Security Officer

Information Security Management

Global Information Security Management

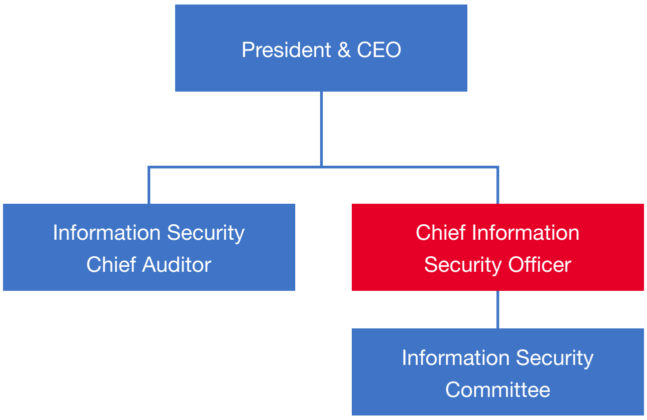
Hitachi Group companies worldwide reinforce their information security in line with our Global Information Security Administration Rules, which conform to the international ISO/IEC 27001 standard. These rules are globally distributed from the parent company in Japan to Group companies worldwide. Other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

Security Monitoring

In Hitachi, the SOC[*1] monitors security on a 24/7 basis so cyberattacks can be detected and countermeasures initiated right away. The IRT[*2] collects and develops security-related data and manages the response to any security incidents.

[*1] SOC: Security Operation Center
[*2] IRT: Incident Response Team

Information Security Promotion Set-up


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

Overseen by CIO until September 2017
CISO position created in October 2017

Preventing Confidential Information Leaks

Hitachi, Ltd. has formulated the Three Principles for Preventing Leakage of Confidential Information to ensure the utmost care is taken with such information and to prevent any leaks or other related incidents.

Three Principles for Preventing Leakage of Confidential Information

Principle 1	In principal, no Confidential Information shall be taken 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.

Hitachi Group companies 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 cyber-attacks, we are creating multilayered controls to prevent leaks of information, including both entry and exit countermeasures.

We also review and investigate the information security status of suppliers based on our internal standards.

Protecting Personal Information

Hitachi, Ltd. has established a personal information protection management system based on the Company's own Personal Information Protection Policy. Hitachi, Ltd. and 44 other Hitachi Group companies* in Japan have received Privacy Mark accreditation.

No customer complaints or claims were received by Hitachi during fiscal 2017 relating to a breach of privacy or loss of data.

As shown by the EU's enforcement of the General Data Protection Regulation (GDPR) in May 2018, consumer privacy laws and regulations are evolving on a global basis. Hitachi is committed to monitoring these trends and taking any appropriate related measures.

* As of May 31, 2018

Information Security Audits

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.

Information security audits are carried out by the Information Security Chief Auditor, an independent appointee by the president of Hitachi, Ltd. There are 221 Hitachi Group companies in Japan that conduct audits in the same way as Hitachi, Ltd., and all results are subject to review. For Hitachi Group companies outside Japan, we use a "common global self-check" approach.

An annual review of Personal Information Protection and Information Security Management is conducted as part of the voluntary inspection of business unit workplaces. We conduct monthly Confirmation of Personal Information Protection and Information Security Management assessments at 693 operations (as of March 2018) that handle important personal information. This regular control mechanism ensures ample safety management and implementation.

Education on Information Security

Annual e-learning programs are held on information security and personal information protection for all directors, employees, and temporary employees. Nearly all of the roughly 40,000 employees of Hitachi, Ltd. participate in these programs. We also offer varied educational courses on information security with different goals tailored to specific target audiences. In 2012, we began simulation training to educate employees about e-mail phishing and other targeted malicious cyberattacks. In the exercise, employees are sent actual examples of malicious e-mails to heighten their awareness of security through direct experience.

Cybersecurity: A Key Management Issue

Damage was caused to some Hitachi systems in May 2017 following an infection with WannaCry ransomware*[1]. Treating this as a management issue, Hitachi is reinforcing cybersecurity measures based on the lessons learned from this incident.

Initial Response to Ransomware Infection

The incident originated around 10 PM JST on May 12, 2017, when systems inside a datacenter began operating unreliably. An investigation for suspected systems failure proceeded, but it was not known at this initial stage that the cause was infection due to a software virus. Once ransomware infection was confirmed about an hour later, the information was reported promptly to the internal Incident Response Team (IRT) and work began to characterize the attack and assess related damage.

Shortly after 1 AM JST on May 13, the IRT concluded from its initial assessment that the incident was due to infection by WannaCry ransomware. This was reported to management, and countermeasures were initiated to prevent more widespread damage. Instructions for urgent countermeasures were developed for the entire Hitachi Group by around 5 AM JST. An Emergency Response Center was set up at Hitachi's head office at 9 AM JST. Work began to assess and repair the damage to systems, and to analyze the route of infection.

Lessons from the Incident

Hitachi drew four lessons from the response to this ransomware infection incident.

First was the threat from cyberattacks that diffuse rapidly within a network. Equipment connected to the company intranet includes not only PCs, servers, and other office equipment, but also equipment used in product development, production facilities, and other OT equipment. In this case, damage spread due to rapid diffusion over the intranet after the virus had infected weak links in the security chain, including office equipment not automatically updated with security patches*[2] as well as OT equipment that would not ordinarily be updated in this way.

The second lesson was the importance of thorough security measures for servers and other office equipment. The systems that were damaged by the infection were ones where security patches had not been installed in a timely manner because system operation precluded their necessary shutdown.

The third lesson related to the difficulties involved in security measures for OT equipment, which in many cases had been designed without considering the need to install security patches or undertake post-installation system updates.

The fourth lesson concerned the need to upgrade business continuity planning to combat the threat from cyberattacks. As with a natural disaster, the assumption with ransomware and other cyberattacks must be that there is no absolute safety, and the approach in an emergency should be to contain the damage and focus on how quickly operations can be restored. The BCPs must envision worst-case scenarios and stipulate related procedures and training so that frontline personnel are better prepared.

Besides the various technical aspects, the management response to this kind of issue must include a comprehensive risk assessment and related decision-making from a business continuity perspective.

The threats in the information security sphere continue to grow year after year, with increasingly sophisticated cyberattacks supplementing problems due to human error, internal misconduct, and changing business conditions, among other factors. The business impact when these incidents occur is significant. Going forward, viewing information security as a critical management issue, Hitachi will seek to reinforce cybersecurity measures and improve systems durability while maintaining an appropriate balance with organizational, misconduct, and system-related factors.

*[1] Ransomware is a type of software virus that places restrictions on an infected computer before demanding monetary compensation in exchange for lifting these restrictions.

*[2] Security patches are programs designed to rectify any faults or weaknesses that are discovered in computing software.

Engaging with Climate-Related Risks and Opportunities

Hitachi sees climate change risks and opportunities as important management issues. One governance mechanism that we established to address such risks and opportunities is the Executive Sustainability Committee, chaired by Hitachi's President & CEO, with other top executives serving as committee members. The committee develops business strategies to minimize risks and maximize opportunities from climate change in line with relevant global regulations and policy trends.

In 2017, the Task Force on Climate-related Financial Disclosures (TCFD), established by the Financial Stability Board in response to a request from the G20 Meeting of Finance Ministers and Central Bank Governors, published its recommendations seeking corporate disclosures of information about climate-related risks and opportunities. In June 2018, Hitachi announced its endorsement of the TCFD and is preparing its information disclosure based on its recommendations. As regards climate-related risks and opportunities, Hitachi is reviewing its risks in two categories, namely, (1) risks related to the transition to a low-carbon economy, and (2) risks related to the physical impact of climate change in accordance with the categories outlined in the new global TCFD recommendations. In terms of opportunities, we are positioning our contributions to the creation of a low-carbon society through enhanced energy-saving features of our products and services as a major opportunity, and are discussing how we can further expand it.

Risks in Transitioning to a Low-Carbon Economy

Policy and Legal

Carbon taxes, energy consumption taxes, emissions trading systems, and other measures may be newly introduced or further strengthened, representing risks impacting directly on management costs in addition to those incurred in complying with the environmental regulations and policies of countries and regions around the world.

To mitigate such risks, we have been reducing or minimizing cost burdens by enhancing production efficiency and introducing energy-saving measures. In fiscal 2017, our energy-saving investments totaled approximately 5.4 billion yen. Should our products fail to meet energy-efficiency standards and regulations, we will risk losing sales opportunities. In addition to strictly complying with existing standards and regulations, we will always endeavor to keep abreast of trends in laws and regulations and participate in the planning of new policies.

Technology

To reduce CO_2 emissions caused by the use of our products and services by our customers, which make up a significant share of emissions in the value chain, we need new technology to achieve further energy-saving in our products and services.

Therefore, by applying Environmentally Conscious Design Assessments in the design and development stages of Hitachi products and services, we assess various environmental aspects at each stage of the product life cycle and strive to minimize environmental impact. In addition, by combining Hitachi's longstanding expertise in a wide range of social infrastructure technologies with OT (operational technology) and IT, we can provide optimal solutions that lead to the creation of new business opportunities.

Market and Reputation

A company's approach to climate change issues influences stakeholders' evaluations, and changes to market values, such as placing great importance on climate change countermeasures, affects customers' choices of products and services. This may pose a risk to business continuity. Hitachi upholds long-term environmental targets of reducing CO_2 emissions throughout its value chain by 50% in fiscal 2030 and 80% in fiscal 2050 compared to fiscal 2010 levels. Measures to attain these goals include investing in new facilities and equipment with higher energy efficiency and targeting greater efficiency in production through digitalization.

Risks Related to the Physical Impacts of Climate Change

Acute and Chronic

Climate-related physical risks include acute risks, such as increased severity of typhoons and floods, and chronic risks, including climate patterns that may cause the sea level to rise and chronic heat waves. Hitachi has a worldwide business presence and believes that disasters due to weather phenomena attributed to climate change, such as increasingly bigger typhoons and torrential rainfall, pose a risk to business continuity.

In order to minimize these risks, we take into consideration such factors as location and the possibility of damage from flooding when setting up a new plant or deciding on the deployment of equipment. We also use the *Hitachi Group Guidelines for Developing Business Continuity Plans* that outline measures to be taken in times of disaster to mitigate risks.

Climate-Related Opportunities

Resource Efficiency

Hitachi is promoting the efficient use of resources by reducing waste, recycling, and undertaking other measures. Also, for the efficient and sustainable use of natural resources, we are promoting efforts to minimize the amount of natural resources we use through improvements in production processes and resource-conserving designs.

Energy Source

Hitachi proactively uses renewable energy for our factories and offices. In our factories, we are able to efficiently use the electricity supplied from photovoltaic power generation facilities, despite fluctuations in the amount of power generated, by monitoring and controlling energy usage on production lines and by using storage batteries. Also, we are promoting the adoption of renewable energy credits and the expanded deployment of internal carbon pricing and the self-consumption solar power generation. In our offices, too, we are enhancing the efficiency of lighting and air conditioning, as well as visualizing energy usage and optimizing the amount of energy used in the building as a whole through Building and Energy Management Systems (BEMS).* In our business operations, we create new business opportunities, such as by actively providing renewable energy from wind power generation systems.

Products, Services, and Markets

Products and services featuring innovative, energy-saving technology that can contribute to the mitigation and adaptation of climate change are viewed as having the potential to increase market value and revenue. Many of our products use energy, so we must enhance the efficiency of our products and services and facilitate low carbonization in order to contribute to resolving the issue of climate change. To this end, we are developing ultra-efficient products and low-carbon energy, as well as encouraging their use. We are also promoting the development of innovative devices and materials that contribute to reducing the environmental burden. In fiscal 2017, Hitachi's total investment in R&D was 332.9 billion yen, including sizable spending to reduce the environmental burden.

A company's approach to climate change issues influences stakeholders' evaluations and affects customers' choice of products and services. Hitachi not only meets the required standards and regulations for the energy efficiency of its products, but also develops and provides energy-saving products and services that go beyond the prescribed standards, thereby increasing opportunities to be chosen by customers.

Resilience

We have devised a plan for vital functions to be maintained through the use of renewable energy and storage batteries if a power outage occurs in any of Hitachi's main factories.

In our business operations, we are providing disaster-prevention solutions to help various countries and regions deal with the rise in natural disasters. Hitachi uses sophisticated IT developed over the years to analyze and evaluate data pertaining to people's daily lives, meteorological and other natural trends, and the operation of social infrastructure, in promoting the provision of solutions conducive to responding to climate change.

* BEMS aim to optimize the internal environment of a building and its energy efficiency.