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

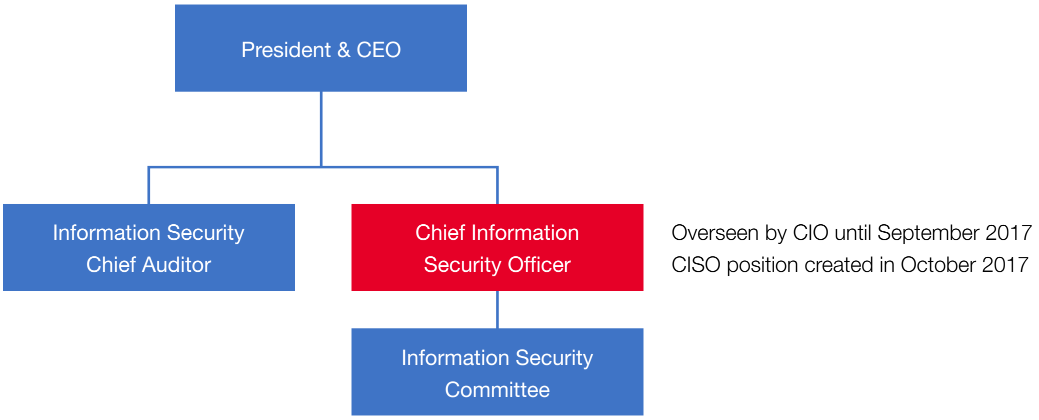
Hitachi Group companies worldwide reinforce their information security in line with our Global Information Security Administration Rules, which conform to the international ISO/IEC 27001 standard. These rules are globally distributed from the parent company in Japan to Group companies worldwide. Other 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.