Promoting Information Security

Information Security Policies

Connectivity is increasing as internet of things (IoT) technology develops, giving rise to new value. At the same time, increasingly intricate cyberattacks that previously targeted IT systems are widening their target range to include IoT and operational technology (OT). Managing information security risks is one of the most critical issues for companies that aim to minimize the risk of business disruption caused by factors such as leaks of information or operational stoppages.

Under these conditions, Hitachi is expanding its Social Innovation Business while practicing information security governance from the standpoint that efforts aimed at strengthening cyber security measures are a key management issue in terms of both value creation and risk management.

Information Security Framework

Previously at Hitachi, Ltd., the CIO[*1], assumed responsibility for, and authority over, the implementation and application of information security and personal privacy protection measures. The CIO was also responsible for the formulation of information tactics in line with management strategies, as well as IT investment policy. However, we appointed a new CISO[*2] in October 2017 in an effort to strengthen and consolidate information security governance throughout the Hitachi Group. The CISO promotes information security for all of Hitachi's products and internal facilities. The CISO also serves as chairperson of the Information Security Committee, which determines policies and measures related to information security and informs all Hitachi Group business sites and companies. Subsequently, these policies and measures are implemented in the workplace by information security officers.

*1 CIO: Chief information officer
*2 CISO: Chief information security officer

Information Security Management

Information Security Management

We have established Global Information Security Administration Rules that conform to the international ISO/IEC 27001 standard and are globally promoting an ongoing information security management system to strengthen our information security management. Previously, these relevant policies had been distributed from the parent company in Japan to Group companies worldwide. However, starting in fiscal 2019, we have begun to further augment our security globally by stationing information security experts in the Americas, Europe, Southeast Asia and China.

Security Monitoring

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

*1 SOC: Security Operation Center
*2 CSIRT: Computer Security Incident Response Team

Preventing Leaks of Confidential Information

Hitachi, Ltd., pays careful attention to the handling of confidential information to prevent leaks and other related incidents.

Specific measures aimed at preventing information leaks include PC encryption, access control and ID management through the establishment of an authentication infrastructure and the creation of multi-layered (entrance and exit) cyberattack defense measures.

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 its own Personal Information Protection Policy. Furthermore, Hitachi, Ltd. and 42 other Hitachi Group companies* in Japan have received Privacy Mark accreditation and are working to safeguard personal information.

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's GDPR initiatives include identifying which operations are impacted by GDPR, evaluating risks, implementing safety management in response to these risks and providing relevant training to all employees.

*As of March 31, 2019

Information Security Audits

Information security audits are independently carried out by the information security chief auditor, who is appointed by the president and CEO of Hitachi, Ltd. Hitachi Group companies in Japan conduct audits in the same way as Hitachi, Ltd., which reviews all results. For Hitachi Group companies outside Japan, we use a "common global self-check" approach. These audits and self-checks are conducted annually at all departments and Group companies.

Information Security Education

Hitachi holds annual e-learning programs concerning information security and personal information protection for all directors, employees and temporary employees. 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.

Fostering a Security Ecosystem aimed at Raising Cyber Security Resilience

Fostering a Security Ecosystem as a New Security Strategy

Recently, cyberattack techniques are becoming more sophisticated than ever before. Cyberattacks are also increasing in number and their range of targets is steadily expanding. Hitachi has launched a new strategy for responding these threats. This strategy involves the construction of a security ecosystem.

The word “ecosystem” describes a state in which plants, animals and the environments in which they live depend on each other to maintain and preserve their own ecologies. As we applied this way of thinking to security, we came to the conclusion that mutual cooperation between departments, even if their operations do not appear to be related, with the common goal of conducting security activities will ultimately enable the maintenance and expansion of business activities throughout all of our organizations.

"Connection" [Tsu-Na-Ga-Ru] within the Security Ecosystem

1. Between Things

In Japan, Society 5.0*1 has been established as an ideal future society for which we should all aim. Once attained, this society will create new value and resolve social issues through a variety of connections. To make Society 5.0 and these connections a reality, our environment will become one in which things such as devices and systems connect with each other, as represented by the IoT.

In May 2017, Hitachi was infected by WannaCry ransomware*2. This infection was the result of testing equipment that was not maintained with an “awareness regarding the necessity of security countermeasures” and had an impact on all Hitachi locations worldwide. Although we had already been applying security countermeasures to internal IT environments, this incident taught us about the additional need for security countermeasures in production and manufacturing areas that had previously been insular.

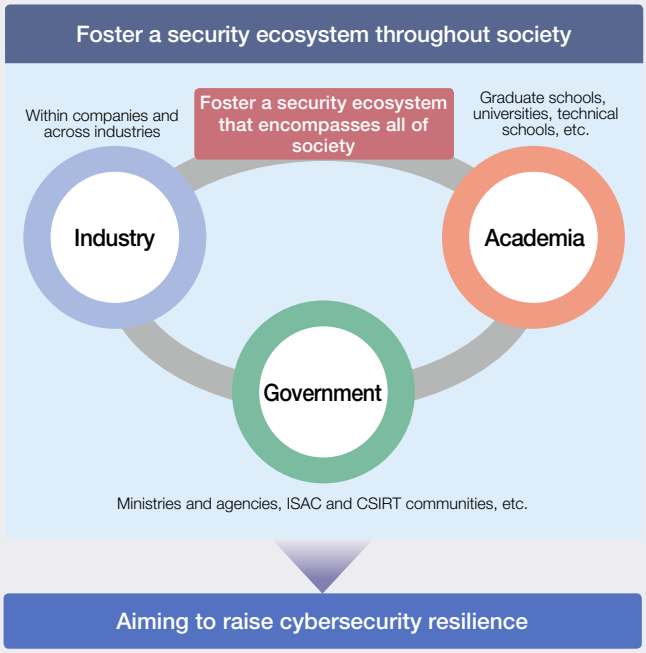
Under these conditions, Hitachi has launched comprehensive global cybersecurity countermeasures (formulated principles and guidelines specific to each environment, etc.) that will cover all types of environments as a wide range of things develop interconnectivity.

2. Between People and Organizations

Moving forward, all corporate business units must mutually cooperate to connect things that had previously been separate while also ensuring security. To support this goal, we are regulating adherence to countermeasures and are holding seminars and workshops targeting communication that transcends organizational and positional barriers. These efforts help us promote activities that connect people and organizations by reigniting awareness regarding individual roles and intensifying cooperation between employees working in the same environments.

3. Within Society

These connections will not be confined to Hitachi. We believe in the necessity of forming communities in which industry, academia and government working to promote cybersecurity transcend established frameworks to share important data, such as information regarding threats and issues faced when implementing countermeasures. Accordingly, Hitachi has proactively launched activities aimed at relating society. Examples of these activities include companies and organizations applying the expertise they acquire from the aforementioned communities to their own security management cycles and further expansion of data sharing.



Aiming to Raise Security Resilience throughout Society

In pursuit of Society 5.0 and to raise cybersecurity resilience*3, Hitachi will promote to foster a security ecosystem that encompasses society in its entirety, enabling people to live more safely and securely. We will construct this ecosystem through cooperation within the corporate world, as well as collaboration with industry, academia and government.

*1 Society 5.0: According to the Cabinet Office website, Society 5.0 is a society centered on people that simultaneously supports economic development and the resolution of social issues through the high-level merging of cyber space (virtual space) with the real world (real space).
*2 Ransomware: A type of computer virus that places certain limits on computer systems following infection and demands monetary or other compensation in exchange for their removal
*3 Resilience: The ability of organizations to adapt to complex and changing environments (from JIS Q 22300, an industrial standard released by the Japanese Standards Association)