Risk Management

Cybersecurity

MHI Group, which provides critical infrastructure to society, recognizes cybersecurity risk as one of its most important risks. With this in mind, we established a cybersecurity basic policy and a cybersecurity strategy.

The Group regularly monitors this risk. The President and CEO supervises the cybersecurity strategy, and the CTO reports the results of discussion in the Cybersecurity Committee at least once a year to the Executive Committee and Board of Directors. Based on the policy and strategy, a cybersecurity program has been implemented under the control of the CTO to minimize the risk of cyber incidents. Cybersecurity governance, incident response, and education and training are maintained and performed under this program. At the same time, we are contributing to the establishment of a global cybersecurity framework.

Cybersecurity Governance

Based on the NIST CSF 2.0[1], MHI Group has established cybersecurity standards and implemented multilayered defense measures against cyberattacks. We also perform periodic self-assessments and internal audits.

Emergency responses are taken immediately and without hesitation when signs of a security risk are found. Furthermore, we are revising standards based on the Group's issues by referring to the state of formulation and revision of guidelines by governments and organizations, such as the Cybersecurity Management Guidelines announced by the Ministry of Economy, Trade and Industry. With respect to control systems for our products and services, we have built a framework that controls cybersecurity risk and will work with business partners to upgrade the cybersecurity capabilities and capacity of our products and services on a regular basis. By driving the development of next-generation cybersecurity solutions, we will help build a safe, secure society.

1 NIST CSF 2.0: National Institute of Standards and Technology Cyber Security Framework 2.0

Response to Cybersecurity-Related Incidents

In the event of a cybersecurity incident, a SIRT (Security Incident Response Team) immediately reacts to the incident, handles analysis and examination of the incident, recovers systems, and carries out further preventive measures. Incidents are reported to stakeholders as needed, including concerned government agencies. Serious incidents are internally reported to directors, and measures are taken in accordance with our crisis management system to swiftly recover operations according to our business continuity plan.

Due to the increased frequency of ransomware attacks requiring swifter management decisions and communication, we confirm and revise the response capabilities and issues of organizations in an emergency through incident response drills that include management.

Cybersecurity Education and Training

MHI Group regularly provides cybersecurity education and training to all employees as warranted by their respective roles with the aim of maintaining and improving their cybersecurity literacy. We also aim to cultivate engineers capable of both safety- and security-minded product and service development.

Contributing to the Establishment of a Global Cybersecurity Framework

Through participation in the Study Group for Industrial Cybersecurity[2], the Charter of Trust[3], promotion of the Declaration of Cyber Security Management 2.0, and other cybersecurity initiatives, MHI Group is contributing to the establishment of a global cybersecurity framework.

2 An initiative by the Ministry of Economy, Trade and Industry to examine industrial cybersecurity measures.

3 An initiative by private corporations to build trust in cybersecurity.

Compliance

MHI Group attaches importance to complying with applicable laws and social norms and is promoting fair and honest business practices. For the promotion of such practices, we established the Compliance Committee, which is chaired by the General Counsel (Senior Vice President). The Compliance Committee draws up and implements Group-wide compliance promotion plans and confirms their progress. In addition, the Committee works to strengthen compliance on a continuous basis through such means as sharing compliance-related initiatives and cases within the Group.

In addition, we have set up whistleblowing hotlines in Japan and overseas in an effort to swiftly respond to various compliance-related risks, including compliance violations or actions that run the risk of becoming compliance violations.

As a global organization, the Group employs thousands of individuals from different backgrounds, nationalities, and cultures. Such diversity of talent and perspectives is one of our greatest assets. Having diverse backgrounds, it is important to work together and promote our business under a common corporate culture.

To that end, we have formulated the MHI Group Global Code of Conduct. Through such efforts as education through e-learning and the distribution of booklets, we strive to disseminate this code of conduct among our employees around the world. At the same time, we have formulated the Compliance Promotion Global Policy, clarifying basic matters and rules for promoting compliance, such as the organizational framework, roles, and administration standards.

Number of Whistleblowing Cases (Cases)

	FY2023	FY2024
Labor and the work environment	87	72
Overall discipline and breaches of manners	27	21
Transaction-related laws	35	44
Consultations and opinions	1	1
Others	13	3
Total	163	141