Cybersecurity

Providing a large number of critical infrastructures to society, MHI Group has established a cybersecurity basic policy and strategy to protect business information (including intellectual property, technical information, sales information, personal information, etc.) and maintain secure operation. Recognizing cybersecurity as a critical risk, MHI Group regularly monitors it as part of materiality initiatives. Our President and CEO supervises the cybersecurity strategy and our CTO reports the results of discussion in the Cybersecurity Committee in a timely manner 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 risks of cyber incidents. Cybersecurity governance, incident response, and education and training are maintained and performed under this program. At the same time, MHI Group is contributing to establish a global cybersecurity framework.

Cybersecurity Governance

MHI Group has defined its internal cybersecurity standard according to the NIST-CSF*1 providing a defense-in-depth mechanism as well as threat detection and prevention by tracking and remedying cybersecurity risks utilizing multiple external intelligence services and other resources. Emergency responses are taken without hesitation when signs of a security risk are found. To maintain and improve our cybersecurity, MHI keeps abreast of the latest cybersecurity intelligence through such measures as vulnerability testing and collection/analysis of threat information. Meanwhile, MHI seeks to raise security awareness of employees by providing education and training, and also performs periodic self-assessments and internal audits. Furthermore, we are revising standards based on MHI Group's compliance and issues by referring to the state of formulation and revision of guidelines by governments and organizations such as the Cybersecurity Management Guidelines*2. For the industrial control system of our products and services, MHI Group has 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 development of next-generation cybersecurity solutions, MHI will help to build a safe, secure society.

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

*2 Published by the Ministry of Economy, Trade and Industry of Japan in December 2016.

Response to Cybersecurity-Related Incidents

In the event of a cybersecurity incident, a CSIRT (Computer Security Incident Response Team) immediately reacts to the incidents, handles analysis and examination of the incidents, recovers systems, and carries out further preventive measures. The incidents are reported to the authorities and 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 according to business continuity planning. 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.

Cybersecurity Education and Training

MHI Group regularly provides cybersecurity education and training to all employees as warranted by their respective roles in the aim of maintaining and improving their cybersecurity literacy. MHI aims to also 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*3, the Charter of Trust*4, promotion of the Declaration of Cyber Security Management 2.0 (announced in October 2022), and other cybersecurity initiatives, MHI Group is contributing to the establishment of a global cybersecurity framework.

*3 An initiative by the Ministry of Economy, Trade and Industry to examine industrial cybersecurity measures. MHI joined this initiative in December 2017.

*4 An initiative by private corporations to build trust in cybersecurity. MHI participated in this initiative in April 2019.