Efforts toward Cybersecurity

Providing a large number of critical infrastructures to society, MHI Group recognizes its responsibility in protecting business information (including intellectual property, technical information, sales information, personal information, etc.). To fulfill this responsibility, MHI has established a cybersecurity policy and strategy to ensure and enhance our cybersecurity. Recognizing cybersecurity as a critical risk, President and CEO supervises the cybersecurity strategy and CTO reports 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 risks of cyberattacks. Cybersecurity governance (establishing standards, implementation of measures, self-assessments, and internal audits), incident response, training and awareness, etc., are performed under this program. At the same time, MHI Group is contributing to the establishment of a global framework.

Cybersecurity Governance

MHI Group has defined a cybersecurity standard according to the NIST-CSF*1 providing a multi-layer protection mechanism as well as threat detection and prevention. Vulnerability test and analysis of collected threat information have been implemented to maintain and improve cybersecurity. Periodic self-assessments and internal audits are also performed to examine the compliance of security measures against MHI Group cybersecurity standard. Through these activities, MHI Group is gaining intelligence of the latest cybersecurity threats which are becoming more sophisticated every day. In addition, industrial control systems provided in MHI Group products are secured through the implementation of a framework that controls cyberrisks for control systems. Furthermore, MHI Group will continue enhancing and developing next-generation solutions in this area.

*1 National Institute of Standards and Technology Cybersecurity Framework

Response to Cybersecurity-Related Incidents

In the event of a cybersecurity incident, a Computer Security Incident Response Team (CSIRT) immediately handles analysis and examination of cybersecurity-related incidents, recovers systems after an incident, and carries out measures to prevent reoccurrence. If necessary, the incidents are to be reported to relevant government agencies and disclosed. Serious incidents are reported to related members including Directors, and measures are taken according to the crisis management system of the company.

Cybersecurity Education

MHI Group maintains and improves cybersecurity literacy among all employees on a regular basis, by conducting cybersecurity education.

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*4, 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. MHI began participation in this initiative in December 2017.

*3 An initiative by private corporations to build trust in cybersecurity. MHI began participation in this initiative in April 2019.

*4 Announced by the Keidanren (Japan Business Federation) in March 2020.