Efforts toward Cybersecurity

Providing a large number of critical infrastructures to society, MHI Group has established a cybersecurity 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 regularly monitors it as part of the materiality initiatives of MHI Group. Our President and CEO supervises the cybersecurity strategy and our CTO reports 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 (establishing standards and rules, implementation of measures, self-assessments, and internal audits), incident response, education and training, are maintained and performed under this program. At the same time, MHI Group is contributing to the global standards.

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. 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 by sharing information and educational content via an intranet portal. Additionally, MHI assesses compliance with MHI Group's cybersecurity standard through periodic self-assessments and internal audits. For our industrial control system products, MHI has built a framework that controls cybersecurity risk. MHI will upgrade cybersecurity capabilities and capacity of our products on a regular basis. By driving

development of next-generation cybersecurity solutions, MHI will help to build a safe, secure society in which people maintain comfortable and convenient lives.

[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 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 other concerned personnel, and measures are taken in accordance with our crisis management system.

Cybersecurity Education

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 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[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 joined this initiative in December 2017.
[3] An initiative by private corporations to build trust in cybersecurity. MHI participated in this initiative in April 2019.
[4] Announced by the Keidanren (Japan Business Federation) in March 2020.