Declaration of Keidanren Cyber Security Management 2.0

October , 2022
Keidanren

In conjunction with the advance of digital transformation (DX) and changes in social and economic activity brought about by the COVID-19 pandemic, cyberspace and physical spaces are merging, not only in industries, but throughout society as a whole. At the same time, damage from cyberattacks is impinging on physical spaces, and there are endless examples of huge impacts on business activities and people's lives. Cyberattacks via supply chains—such as those targeting business partners and overseas subsidiaries—are also on the rise. Moreover, as heightened geopolitical tensions extend into cyberspace, cybersecurity is becoming a crucial domain for national security.

Under these circumstances, from the perspectives of creating value and building value chains aimed at realizing Society 5.0 for SDGs, as well as managing risk, it is no exaggeration to say that effective cybersecurity measures are now a key management priority for all companies.

All businesses will implement cybersecurity measures and contribute to making cyberspace safe and secure. To this end, business leaders pledge to address the following points:

1 Recognize Cybersecurity as a Management Issue

- Enhance their own understanding of the latest cybersecurity circumstances and actively engage in management by positioning cybersecurity spending as an investment essential to promoting DX.
- Take responsibility themselves for cybersecurity measures while recognizing that enhancing cybersecurity throughout the entire supply chain is a critical management issue, addressing risks associated with digitalization, and exercising leadership.

2 Develop Management Policies and Declare Intentions

- Develop management policies and business continuity plans aimed at prompt recovery from security incidents while prioritizing detection, response, and recovery in addition to identifying and protecting against risks.
- Take the lead in declaring companies' intentions to internal and external stakeholders and make every effort to voluntarily disclose recognized risks, and measures to deal with them, in corporate reporting.

3 Build Internal and External Systems and Implement Security Measures

- Ensure sufficient resources including budgets and personnel, establish internal systems, and take necessary human, technical, and physical measures.
- Develop human resources and conduct training required for those at every level, including the management, corporate planning staff, technical specialists, and other employees.
- Manage cybersecurity throughout domestic and international supply chains, including business partners and outsourcing contractors, by utilizing guidelines and frameworks for cybersecurity measures and cooperating with government support programs for such measures.

4 Contribute to Widespread Use of Cybersafe Products, Systems, and Services

- Manage cybersecurity across the full spectrum of corporate activity, including development, design, production, and supply of products, systems, and services.

5 Contribute to Building Safe and Secure Ecosystems

- Collaborate with relevant government agencies, organizations, industry associations, and other bodies to actively share information, engage in dialogue, and build human networks, both in Japan and internationally.
- Contribute to reinforcement of cybersecurity in the entire supply chain and throughout society by raising awareness of measures taken on the basis of such information.