Risk Management

Risk Identification and Countermeasures

The Nitto Group distributes questionnaires on business risks to over 2,000 management-level employees every year. The purpose of this survey is to determine risks concerning the entire Group and those specific to individual businesses and regions, as well as to enhance the level of each management-level employee's risk awareness. Based on the survey responses, we determine what actions are being taken to manage risks at each workplace and discuss anything else that needs to be done at CSR workshops for management-level employees, thereby helping each site and Group company to enhance their risk management. Going forward, we aim to raise the level of risk management of the entire Group by promoting horizontal cooperation among such individually taken measures against business risks.

Reinforcement of Information Security Management

In its efforts to achieve "a state of fewer security incidents*1 and no information leaks" the Nitto Group takes not only tangible technical measures, but also intangible measures, including enhancement of information security systems and continuous employee training through e-learning and other methods.

In fiscal 2017, we began making an effort to further raise the Group's overall level of information security management by monitoring sites and Group companies that reported a less than satisfactory self-evaluation rating in information security management.

To follow up on the surprise e-mail test that was given last year, we gave an advanced test to over 400 IT engineers. This time, we sent out an e-mail that contained seemingly ordinary work instructions to see how the recipients would react to it, which helped us to better understand how they determine whether an e-mail is suspicious and what their initial responses would be if they were to open it for some reason. Together with the findings from the test that we sent out to all e-mail users within the Group last year, we are strengthening our efforts to prevent information leaks by targeted e-mail attacks*2.

*1 Incidents and accidents including data loss, virus infection, and unauthorized access.
*2 A type of cyber attack that attempts to steal information by sending an e-mail with an attached file or URL containing a computer virus to members of a targeted organization.

Business Continuity Management

We at the Nitto Group recognize the importance of a prompt initial response for "disaster mitigation (minimizing damage caused by disasters)" and "quick recovery." Accordingly, we distribute the "Emergency & Incident Reporting Guidebook" to top managers and their acting representatives at all of our sites and Group companies to ensure that any and all emergencies will be reported to Nitto's CEO without delay. We also develop reporting systems and communication infrastructures to allow two-way communications in times of emergency. We also continue to revise restoration plans based on past experiences and issues that come to light during drills.

While constantly updating these systems and plans, we have also formed working groups for each function, including Procurement, Logistics Services, Production, Environment, Safety, and IT in order to have them work on business continuity with the supply chain in mind. In fiscal 2018, we aim to increase the effectiveness of our business continuity plan (BCP) by accelerating initiatives where these working groups act in unison.

Inter-Site Combined Drill by Sales Teams

On November 28, 2017, Nitto's key domestic sales offices in Sendai, Tokyo, Nagoya, Osaka, and Fukuoka, participated in a joint drill in preparation for a major earthquake. In a simulated situation with limited means of communication, they began by ensuring the security of employees and confirming their safety, and then established a disaster countermeasures headquarters, determined the extent of the disaster, and verified the backup system for resuming business. We will conduct such drills on a regular basis to continuously validate and improve the BCP so that we can work in close collaboration with one another when any of our key sites are affected.