Fiscal 2015 Activities Review and Plan for Fiscal 2016

1. The Ricoh Group's Information Security Activities

In response to changes emerging in the social environment, the Ricoh Group is promoting its PDCA management system to boost the information security level. We have revised the Ricoh Group standard rules and the Ricoh Family Group Information Security Measures, and we are providing employees with appropriate education through e-learning, and we are also performing checks and improving information security through internal audits.

Topic in Japan

In Japan, the law to partially revise the Act on the Protection of Personal Information and the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure was enacted on September 3, 2015 and subsequently promulgated on September 9. As a result, the definition of personal information has been made clearer. In the future, the government will set ordinances to provide for the specific treatment of personal information and numbers.

In response to this, the Ricoh Group clearly designated the departments to handle the administration of personal numbers and formulated rules on the treatment of these numbers to be obeyed uniformly by all members of the Group.

Following the promulgation of the aforementioned Act on the Use of Numbers to Identify a Specific Individual, the Ricoh Group has revised its Basic Policy for Personal Information Protection and its policy on the Handling of Personal Information, which can be viewed on the following websites:

Basic Policy for Personal Information Protection:
http://www.ricoh.com/privacy/

Handling of Personal Information:
http://www.ricoh.com/privacy/index_2.html

2. Maintenance of Groupwide Unified ISMS Certification (for ISO 27001)

Since its initial attainment of unified ISMS certification in December 2004, the Ricoh Group has updated its certification status by passing annual audits and triennial renewal audits conducted by a third-party auditor. In fiscal 2015, we were again reviewed for the annual audit and successfully maintained our certification.

As of February 2016, a total of 64 Ricoh Group companies (16 in Japan and 48 overseas) have been certified. TECHNO RENT Co., Ltd. (in Japan) has been audited for an expanded registration scope and newly included in the groupwide unified certification list.

Plan for Fiscal 2016

In fiscal 2016, we will undergo the fourth renewal audits to maintain our certification.

ISMS Certification

3. Continual Improvement and Deployment of Ricoh Family Group Information Security Measures

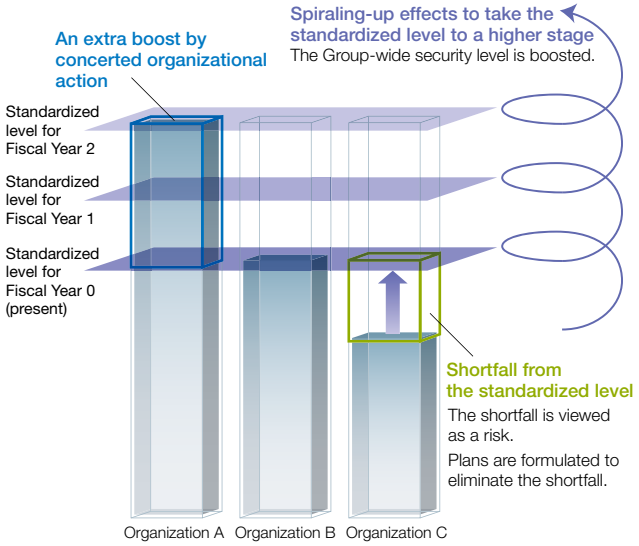
The Ricoh Family Group Information Security Measures were established to maintain the security level of the entire Group and optimize risk assessments. They cover all the rules to be followed by members of the Group.

Based on these measures, a series of control steps have been set for the routine processing of information (specifically, transport, transmission, and the removal of information), thereby making it possible to perform baseline risk assessments. We are also continuously making improvements to respond to new threats and the spread of new IT devices.

In fiscal 2015, we added no new measures to the Ricoh Family Group Information Security Measures. In Japan, we compiled the information security guidelines to explain the related rules and specific examples based on the Security Measures.

Plan for Fiscal 2016

In today's business environment, we often take our tablets or computers with us when we work outside the company. However, computers, unlike thin clients and cloud services, have information stored on their hard disks and such information could fall into the wrong hands if the machines are lost. Recognizing this, the Ricoh Group has since 2013 been fostering hard disk encryption for the notebook computers used by employees to reduce the risks associated with taking computers and any information stored on them outside the company. In fiscal 2016, we will make hard disk encryption mandatory for all the computers taken out of the company by employees and will revise the Ricoh Family Group Information Security Measures accordingly. We will also continue to improve and foster the use of the information security guidelines.



4. Enhancing the Ricoh Group's Business Continuity Plan and Management

Information pertaining to risk management, as part of the governance efforts of the Ricoh Group, is publicly disclosed. For details of our business continuity plan (BCP), please refer to:
http://www.ricoh.com/governance/risk.html

This section focuses on activities on BCP and business continuity management (BCM) related to our IT infrastructure. In fiscal 2015, as in previous years, we conducted contingency drills and worked to improve the BCP systems based on the findings of the drills as part of our efforts to maintain the effectiveness of our BCP.

(1) Drills held in fiscal 2015

	Drill descriptions	Feedback on drill results
1	Drill focusing on initial response to an emergency (Starting with initial response, assessing damage, establishing an emergency command post,and beginning activities at the command post	After the drill, feedback from the participants on the procedures, including written procedures, was collected. Improvement points identified were reflected in the revised written procedures.
2	Drill focusing on checks to confirm the operational status of IT systems in the event of an emergency	Verification was conducted for the presence and appropriateness of the written checking procedures prepared for each system. Where necessary, a request was made to create or revise the relevant written procedures.

(2) Data continuity (backup system)

Simultaneous loss of both primary data in an information system and its backup data would have a critical impact on business continuity. In addition to implementing basic measures, i.e., remote storage of backup data, physical transfer by the transportation of backup tapes as well as creating and storing backups online in a cloud environment have continuously been in place to strengthen data continuity structures. The method to be adopted is determined primarily based on the importance, volume, and update frequency of the backup data.

Plan for Fiscal 2016 (IT Systems)

We will continue to enhance processes both for disaster-prevention measures (*1) and BCP (*2), conduct drills to familiarize employees with the processes, and assess these measures to make further improvements.

1. Assess the implementation status in terms of BCP
2. Conduct periodic drills
3. Strengthen collaboration with domestic affiliates, including the implementation of joint drills.

*1 Disaster-prevention measures: Measures to anticipate disasters and minimize damage

*2 "BCP" stands for business continuity plan/planning, which is aimed at minimizing damage and resuming business activities as soon as possible in the event of a large-scale disaster or accident

5. Continuous Education to Raise Awareness of Information Security Issues

We introduced the subject of "roles and responsibilities required of information managers" into the management training programs provided under the Group's job-grade-specific training system.

We also offered an e-learning program on information security to all Ricoh Group employees. In the program, employees learned about the daily security habits that they are asked to adopt, including the basic handling of information in their business operations (how to manage their computers and email exchanges), as well as rules and warnings regarding the use of social media and cloud services that might give rise to unexpected incidents if not used appropriately.

We also provided some of our official dealers in Japan with online information security education. In addition, we have shared files related to information security education translated into English internally for English-speaking employees. For directors, we once again warned them against the recently increasing targeted email attacks and taught them how to prevent damage that could be caused by such attacks.

With regard to targeted email attacks, we are sharing related information internally to raise awareness among Ricoh Group employees of the importance of not thoughtlessly opening email attachments or clicking on links inside emails as well as the need to keep the operating systems and antivirus software of their devices up to date.

Plan for Fiscal 2016

For new employees, we will implement an e-learning program on information security to replace the information security education traditionally provided as part of the collective education uniformly given by the Ricoh Group.

The e-learning program, which can be taken at their own pace, will help new employees increase their level of understanding about the Ricoh Group's approach to information security and the security-related information and action guidelines that they need to know soon after joining the company. Furthermore, each group company can implement the program at the most appropriate timing according to its own educational schedule.

We will continue to educate all employees on information security by providing them with information and knowledge about the security risks posed by changes in society and the IT environment.

6. Occurrence of Incidents and Prevention of the Recurrence of Similar Incidents

6.1 Incident reporting

In fiscal 2015, we had two major incidents and disclosed information about these incidents outside the company.

(1) Theft of a laptop computer that contained customer information

Measures to prevent the recurrence of similar incidents:

We will enhance our security measures, review and improve the in-house standards, raise awareness among employees of the importance of protecting customer information and other personal information, and carry out internal audits on the handling of information in a stricter manner.

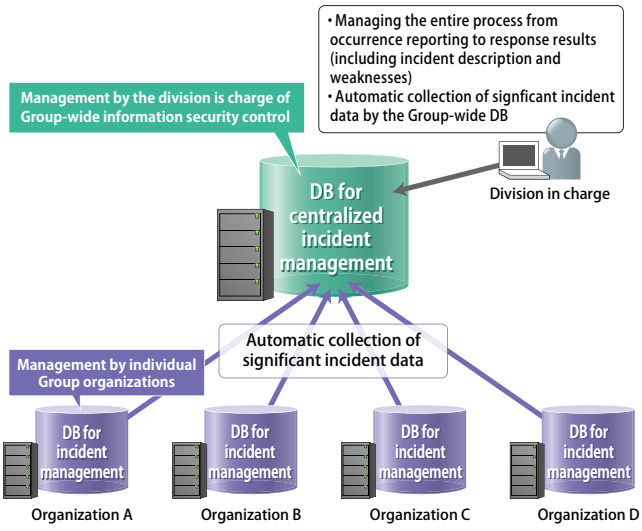
(2) Unavailability of ordinary services due to a system failure

Measures to prevent the recurrence of similar incidents:

The failure was caused by a defect in the driver software of a device that configured redundancy. We replaced the driver software and board with new ones to ensure the normal operation of the system.

6.2 Management of incidents within the Group

We are committed to preventing the occurrence and recurrence of information security incidents within the Group by taking the following steps.



(1) Sharing of information

We have been sharing information on information security incidents and the measures to be taken to prevent the recurrence of similar incidents.

(2) Increasing information security awareness of employees through education
We include incidents that tend to occur in daily operations, such as the loss of computers and external recording media as well as virus infections, in the subjects covered by our information security education with a view to making employees more aware of the measures to prevent such incidents.

(3) Internal auditing
We have incorporated particularly important incident information and educational items as priority items to be reviewed in our internal information security audits in an effort to increase awareness and promote improvements regarding these items across the Group.

(4) Management review
We include incident analysis results in the target of our management review for top executives to check the effectiveness of the measures implemented to prevent the recurrence of similar incidents.

Plan for Fiscal 2016
We will continue to implement measures to prevent the loss of information that might be caused due to the physical loss of computers and external recording media.
As for computer security incidents that might be caused by cyber attacks and others via external networks, the CSIRT (*) will work to achieve early solutions.
Also, to prevent other types of incidents, we will implement management systems, including those to increase employee awareness by way of education, ensure security through internal auditing, and make better use of IT.

* The Computer Security Incident Response Team (CSIRT) is an organization that deals with computer attacks, threats and security incidents arising as a result of connection with external networks.

7. IT Security

We released version 4.0 of the IT Security Guideline, which was first released in fiscal 2014, under the new name “IT Security Requirements.”

At our bases across the globe, we analyzed the gaps between the Requirements (minimum requirements) and the reality, and prioritized the measures to be implemented at each of the bases to narrow the gaps identified at their sites. These measures are incorporated in the action plans and budget allocation plans that we have made for fiscal 2016 and onwards.

In fiscal 2015, an illegal access to the open Internet system implemented by one of our affiliated companies in Asia was identified, but there was no actual damage caused by this incident as a result of the CSIRT (*) having taken appropriate measures against it.

Plan for Fiscal 2016
We will optimize our security measures based on the results of gap analysis and examine the items to be added to the IT Security Requirements.
Moreover, we will analyze the gaps between the Requirements (minimum requirements) and the reality also targeting the affiliated companies engaged in production, with an eye to optimizing the criteria to be met globally across the Group and those to be met separately by each base and in each country for the implementation and operation of IT systems, thereby enhancing the effectiveness and efficiency of our information security activities.

* The Computer Security Incident Response Team (CSIRT) is an organization that responds to computer attacks, threats and other security incidents arising as a result of connection with external networks.