Fiscal 2014 Activities Review and Plan for Fiscal 2015

1. Outline of Fiscal 2014 Activities

In fiscal 2014, a number of major cases of personal information leaks were reported in Japan, spurring public and private organizations alike to re-examine their information management systems as well as impacting the planned revision of the Act on the Protection of Personal Information. The incidents also highlighted the limitations of software-dependent information security measures against the increasing threat of cyberattacks.

At the Ricoh Group, following the occurrence of content altering of a corporate webpage (reported in fiscal 2013), we organized a CSIRT function to accelerate our CSIRT activities, which have been designed to maintain consistency with the previous information security management systems. In fiscal 2014, our CSIRT efforts focused on the deployment of Virtual One IT, the Group's global-level cybersecurity structure.

We maintained the groupwide unified ISMS certification (for ISO 27001) for fiscal 2014. Also, we accomplished the transition to ISO/IEC 27001:2013 (JIS Q 27001: 2014).

To achieve commonality among multiple ISO management system standards, particularly for risk-related concepts, risks have been redefined in more general and abstract terms, seemingly compromising understandability. However, we worked out a simple scheme around key concepts-"information security objective," "risk," "risk source," "event," and "consequence"-based on the premise that an event is the result of a cause.

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

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 2014, we were again reviewed for the annual audit and successfully maintained our certification.

As of January 2015, a total of 65 Ricoh Group companies (17 in Japan and 48 overseas) have been certified. Softcomm Co., Ltd. (in Japan) has been audited for an expanded registration scope and newly included in the groupwide unified certification list.

Also, we accomplished the transition to ISO/IEC 27001:2013 (JIS Q 27001: 2014), a standard revised in fiscal 2013, by passing the annual audit for fiscal 2014. To comply with the latest version, we first carefully examined the revised standards and then reviewed the Ricoh Group standard rules and the Ricoh Family Group Information Security Measures to identify necessary modifications to be made. Determining requirements and controls to be addressed, we drew up specific action plans and communicated them across the Group to be effectively implemented, thereby achieving a swift and efficient transition. This smooth progress was partly facilitated by the fact that many of the newly added control items call for measures that have already been practiced under our Information Security Measures.Following the recent transition to the new standards, we updated ISMS-related software programs, including risk assessment tools.

For the scope of the certification, please refer to the list of Ricoh ISMS registrations (Ricoh Group Registration Scope) prepared by an external certification body.

Plan for Fiscal 2015

In fiscal 2015, we will undergo an annual audit 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. Based on these measures, control items 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 expansion of new IT devices.

In fiscal 2014, we started a new initiative to establish a set of measures required on a global level relating to IT security implementation. As part of the efforts, the IT Security Guideline 1.0 was released, as outlined below. The Guideline has been formulated under our Information Security Measures to provide specific approaches to implement the Measures, that is, “how” to utilize IT to achieve “what” is required by the Measures.

IT Security Guideline

(1) Purpose

The purpose of this Guideline is to establish the minimum security requirements and best practices that must be implemented by each Regional Headquarter division in order to provide adequate and reasonable protections against security incidents.

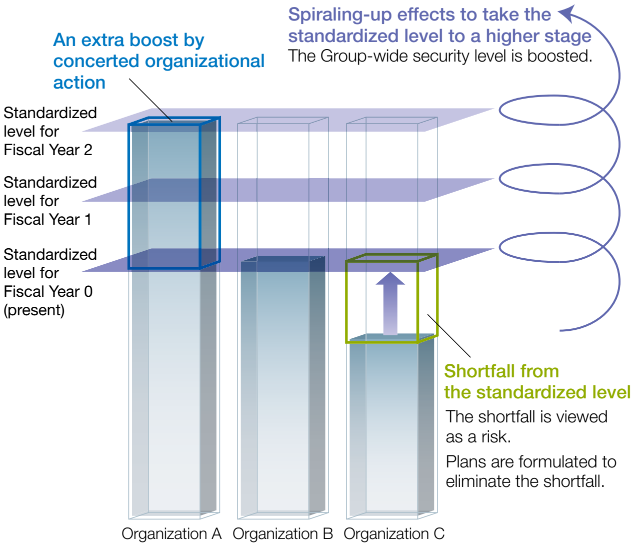
(2) Approaches

■Target scope and systems of the Guideline
■Collection and monitoring of security logs
■Log management
■Removing viruses and detecting malware
■Scanning for Internet vulnerability
■Testing for web applications
and others

Plan for Fiscal 2015

In fiscal 2015, we will assess the IT security implementation status for the Group’s global bases and make revisions to the Guideline as appropriate. In line with this revision, the Ricoh Family Group Information Security Measures will be reviewed.

We will also increase the efficiency of our information security activities by optimizing global and local (national/organizational)-level requirements in terms of both IT implementation and operation.



An extra boost by concerted organizational action
Spiraling-up effects to take the standardized level to a higher stage
The Group-wide security level is boosted.
Standardized level for Fiscal Year 2
Standardized level for Fiscal Year 1
Standardized level for Fiscal Year 0 (present)
Shortfall from the standardized level
The shortfall is viewed as a risk.
Plans are formulated to eliminate the shortfall.
Organization A
Organization B
Organization C

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://jp.ricoh.com/governance/risk.html

This section focuses on activities on BCP and BCM (business continuity management) related to our IT infrastructure. In fiscal 2014, we conducted specific measures to solidify our BCP systems, such as holding contingency drills and improving the BCP systems based on the findings of the drills. We were able to implement such measures because we were in a phase where a solid system was in place to operate the PDCA cycle in a continuous and steady manner.

(1) Drills held in fiscal 2014
The following drills were held during the fiscal year.

	Drill descriptions	Feedback on drill results
1	Drill focusing on initial response to an emergency (Assessing damage, deciding on the necessity of establishing an emergency command post, etc.)	After the drill, participants' feedback 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 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 for stronger data continuity structures. The method to be adopted is determined primarily based on the importance, volume, and update frequency of the backup data.

Reference

Ricoh Industry Company, Ltd., Tohoku Office of Ricoh Technologies Company, Ltd., and PC Unit Products Company of Ricoh Company, Ltd. acquired ISO 22301 for their business continuity management systems (BCMS) and completed their registration in December 2013. The following related information from the Ricoh Group appears on the website of the Ministry of Economy, Trade, and Industry.

■The Ricoh Group's basic policy on BCP and recovery targets and objectives
■Background and objectives of the seminars for suppliers
■Key points in building BCP/BCMS

http://www.meti.go.jp/policy/economy/hyojun/group-ms/index.html (in Japanese)
http://www.meti.go.jp/policy/economy/hyojun/group-ms/c_group_17.html (in Japanese)

Plan for Fiscal 2015 (IT Systems)

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

1. Assess the implementation status for measures adopted for each IT system based on its importance in terms of BCP
2. Conduct periodic drills to familiarize employees with necessary BCP management and implementation processes
3. Strengthen collaboration with domestic affiliates for effective BCP processes, including joint drills for improving processes

Disaster-prevention measures: Measures to anticipate disasters and minimize damage
BCP: Planning and preparation for continuation of important operation

* BCMS: business continuity management system
* BCM: business continuity management
* BCP: business continuity plan/planning

5. Continuous Education to Raise Awareness of Information Security Issues

We offered an e-learning program on information security to all Ricoh-Group employees.

The program called for cautions on a number of important issues, including a renewed warning against transmitting data without permission and installing file-sharing software, practices that entail the risk of confidential information being leaked over the Internet. For the recently increasing targeted email attacks, learners were reminded of the need to be cautious about opening email attachments and clicking on links inside emails as well as the importance of keeping operating systems and antivirus software up to date. Participants were also briefed on common hacking tricks. In addition, in line with the Ricoh Group Social Media Policies, employees were warned about posting messages on social media and the danger of triggering libel or defamation suits involving the Group.

Plan for Fiscal 2015

We will introduce 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. This aims to help managers clearly understand their roles and responsibilities for a range of information management processes, from identifying information to be controlled and establishing handling procedures for the target data to reviewing operation procedures to strengthen safety and security for information use and taking necessary actions in the event of security incidents, thereby achieving adequate information security management for the relevant organization.

We will also provide training for all Ricoh Group employees focusing on disseminating the Group's policies on information security as well as updating the security rules for routine operations to meet changes in the IT environment and privacy-related requirements.

6. Preventing Recurrence of Information Security Incidents

In fiscal 2014, we identified no major computer security incident that required a public announcement or reporting to external auditors and regulators.

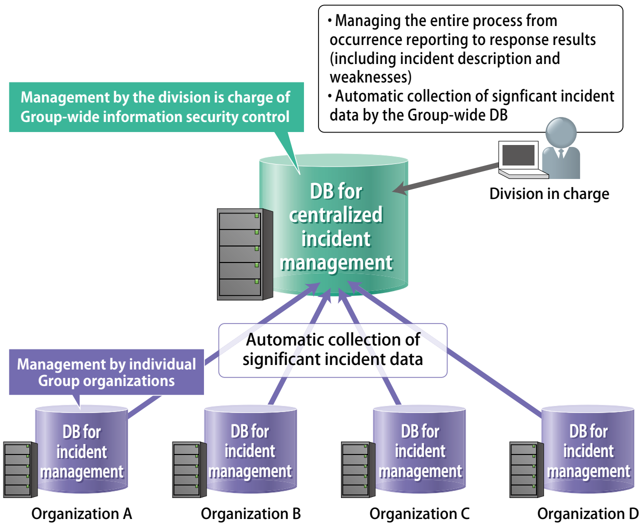
In fiscal 2013, we reported the occurrence of a major incident, specifically, an unauthorized change to part of our website. This incident awoke us to the real threat of cyberattacks and the importance of CSIRT*1 activities, prompting us to take remedial actions employing external support. Still, it took around two months to restore the damaged webpage and resume service provision.

Undergoing the above process, we have developed adequate risk awareness for cybersecurity and started the substantial acceleration of our CSIRT activities to build a global-level security management structure (Virtual One IT).

*1 CSIRT: Computer Security Incident Response Team. An organization that responds to Internet-based computer security incidents and threats.

We operate a management system to prevent the occurrence and recurrence of information security incidents by following the steps specified below:

1. Sharing information on information security incidents and measures taken to prevent their recurrence across the Group. This step has been taken since fiscal 2011.
2. Including incidents that tend to occur in daily operations, such as the loss of computer terminals and external recording media, as subjects for information security education in order to ensure that employees are well aware of the measures to be implemented to prevent the recurrence of similar incidents.
3. Incorporating 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.


• Managing the entire process from occurrence reporting to response results (including incident description and weaknesses)
• Automatic collection of signficant incident data by the Group-wide DB
Management by the division is charge of Group-wide information security control
DB for centralized incident management
Division in charge
Automatic collection of significant incident data
Management by individual Group organizations
DB for incident management
DB for incident management
DB for incident management
DB for incident management
Organization A
Organization B
Organization C
Organization D

Plan for Fiscal 2015

We will work to maintain the status of zero serious incidents.

Also, following the completed transition to ISO/IEC 27001:2013 (JIS Q 27001: 2014), we will comprehensively revise our incident management systems based on the new risk management scheme, including redefining incidents and re-establishing escalation rules.

Particularly for Internet-based computer security incidents, or cyberattacks, we will work to ensure that the CSIRT functions readily in the event of an incident by in helping the affected organization solve the problem promptly and effectively. For overall information security incident management, we will implement our management system effectively, raising employee awareness through education and promoting verification and improvement through internal auditing while utilizing IT to prevent occurrence and recurrence of incidents.

7. CSIRT Activities through Virtual One IT (new reporting item)

Following the cyberattack incident that affected us in fiscal 2013, we organized a CSIRT and developed it into a global function in a short time. (Details are provided above in “6. Preventing Recurrence of Information Security Incidents.”)

Goal for Fiscal 2014

We aim to build a global-level structure for promoting computer security incident management, assigning personnel from various locations and divisions of the Groups global bases (Virtual One IT). The management structure will focus on functionality in three areas: prevention, early detection, and swift response.

In fiscal 2014, we identified no major computer security incident that required a public announcement or reporting to external auditors and regulators.

The Ricoh Global Security Summit was held in Munich, Germany from September 23 to 25, 2014. Details are provided at:

http://jp.ricoh.com/security/management/news/news_004.html (in Japanese)

http://www.ricoh.com/security/management/news/news_004.html (in English)

We established a global emergency contact network and formulated an annual plan for CSIRT activities.

Plan for Fiscal 2015

We aim to start operating the global CSIRT using the Virtual One IT structure based on the established global contact network. In relation to this, we plan to develop a structure to increase cooperation between CSIRT and PSIRT[*2] activities, aiming to achieve more consistent information security management. We will also release the IT Security Guideline 2.0.

[*2] PSIRT: Product Security Incident Response Team. An organization that responds to product-related security incidents and threats.