[News] Organization of the Ricoh Global Security Summit

The Ricoh Global Security Summit (hereinafter "the Security Summit") was held in Munich, Germany for three days from September 23 to 25, 2014.
A total of 15 people from around the world participated in this meeting—five from Japan, three from the Americas region, five from the European region, and two from the Asia-Pacific region (including three in Japan and another three in Europe by teleconference).
The participants, who comprise the Ricoh Group's major members in charge of information security, engaged in discussions about information security, exchanging opinions on information security-related issues and requirements from a global viewpoint.

1. Agenda of the Security Summit

At the Security Summit, participants initially shared information on each region's information security situation and associated issues, followed by examination of the following items.

(1) Internet Security
  1) Security of the basic OS, network devices, and online servers
  2) Security of online applications
(2) Global CSIRT
  1) Framework to support the global CSIRT
  2) Roles and responsibilities of the global CSIRT
  3) Scope and responsibilities of the global CSIRT
  4) Exchanging information and making educational plans for the global CSIRT
(3) Global Security Guidelines
(4) Requirements to Ensure Data Access
(5) Future Management of the Security Summit

Venue of the Security Summit held in Munich, Germany and participants in the Summit

2. Detailed Examination of the Global CSIRT

Participants spent much time examining the CISRT with a view to establishing a globally consistent security management system and forming appropriate responses.

(1) Definition of Terms with Regard to Responses to Global Incidents

Participants defined terms such as "CSIRP*1," "CSIRT*2," "incident," "event," "vulnerability," and "War Room" (physical and virtual operations headquarters).

(2) Roles and Responsibilities in Responding to Global Incidents

Roles and responsibilities were clarified for the following categories based on function and for the head office as well as each region.

1) Prevention

Roles and responsibilities, including formulating global incident response plans, testing and reporting vulnerabilities, providing education on the response to incidents, utilizing information concerning threats, and collecting system information

2) Detection (recognition, analysis and notification phases)

Roles and responsibilities, including monitoring and log acquisitions

3) Responses (control, elimination and recovery phases)

Roles and responsibilities, including suspending systems and services, documentation, using the emergency contact network, and providing emergency support

4) Post-incident phase

Roles and responsibilities, including evaluating responses to incidents to prevent their recurrence

5) Guidelines and rules

Roles and responsibilities, including establishing security guidelines and rules

(3) Examination of workflows to respond to global incidents

For responses to global incidents, seven phases were defined, from the detection of a global incident to the post-incident phase, and participants examined the workflows and the following items for each of the phases:

1) Human resources and their skills
2) Processes
3) Technologies and tools

3. Results of Examinations Conducted at the Security Summit

As a result of their examinations, participants in the Security Summit reached a global agreement on the following initiatives:

- Role-sharing on the global CSIRT and a workflow to deal with incidents
- Publication of the guidelines showing the standard IT security implementation level, and future expansion of the target areas
- Annual examination process for the establishment of IT security based on cooperation between regions

4. Conclusion

It took up to three months to prepare for the first round of the Security Summit, including preparations for organization of a regular meeting with each region through the use of the UCS*3.

For each item on the agenda, participants in the Security Summit conducted specific examinations, which resulted in enhancing global information security and fostering mutual communication on a global level. Through the discussions, participants confirmed the global standardization policy for information security and agreed on the future organization of the Security Summit.

The Security Summit was one of the most important initiatives to be worked on by the Ricoh Group in a virtual and global manner. In the past, the head office formulated the measures and dispatched related information to the Group's bases around the world for local implementation.

To lead Ricoh's large organization, global headquarters makes use of top human talent and skills as well as sophisticated processes, and implements the latest technologies and tools.

The Ricoh Group has now built up a global process model. Proposals and comments made at the Security Summit will be summarized and dispatched across the Group for local implementation of related measures.

The Ricoh Group will continue to improve the quality and efficiency of measures against information security incidents on a global scale.

*1 CSIRP: Computer Security Incident Response Plan
*2 CSIRT: Computer Security Incident Response Team
*3 RICOH Unified Communication System:Ricoh's portable terminal for remote communication
http://www.ricoh.com/ucs/