RICOH
imagine. change.

Information Security Report 2022

Message from top management

RICOH Company, Ltd.

General Manager, Information Security Management Center

Hiroyuki Teshima

Risks associated with information security have been increasing rapidly in recent years. The scope of corporate response is also expanding due to the frequency of cyber attacks, the diversification and sophistication of malicious technologies (ransomware, etc.), the strengthening and diversification of regulations in various countries, and the emergence of geopolitical risks.

Additionally, as our management goal is to transform into a digital services company, we need to place "security" as a corporate value not only to mitigate geopolitical risks in digital services, but also to further solidify profitability in our existing businesses.

The Ricoh Group has been transforming into a digital services company, and in 2021, we launched data business in earnest with the release of the "AI at Work" series, a new service that uses proprietary natural language processing AI (artificial intelligence) and other technologies to support business operations.

At the same time, we established the Information Security Management Center to make quick management decisions on company-wide (Ricoh Group) information security, clarify strategies to comply with the laws and regulations of various countries, and link security to the enhancement of corporate value.

In recent years, as companies have been aiming to improve their corporate competitiveness through digital transformation (DX), security issues that need to be resolved have also arisen.

In light of this social situation, the Ricoh Group aims to become a company that continues to be trusted by society by taking measures against increasingly sophisticated cyber attacks, ensuring high-quality security of products, systems, and services through "security by design," and promoting information security measures throughout the supply chain.

We hope that you will read this report, which presents an overall picture of the Ricoh Group's information security initiatives.

Index

Message from top management 1

1 Introduction 4

1-1 Background and importance of initiatives in information security 4
1-2 Positioning of information security in management 5

2 Ricoh's information security initiatives 6

2-1 Concept of information security 6
2-2 Information Security Basic Policy/Individual policies 6
2-3 Security organization 6-7
2-4 Scope of information security 8-9

3 Product security 10

3-1 Basic policy on information security for products and services 10
3-2 Pursuit of safe and secure products 10
3-2-1 Security by design 10
3-2-2 Bringing attention to security risks 10
3-3 Ricoh's layered approach to security 11

4 Corporate security 12

4-1 Ricoh's corporate security strategy 13-14
4-2 Enhancing security incident response 15
4-3 Security training 15

5 Data privacy 16

5-1 Protection of personal information 16
5-2 The Ricoh Group's Data Privacy Policy 17
5-3 The Ricoh Group's Basic Policy for AI Technology Utilization 17

Conclusion 18

Basic Info

Purpose

The purpose of this report is to explain the Ricoh Family Group's information security-related activities to stakeholders.

Reporting period

2021/7/1~2022/9/30

Report Scope

Ricoh Family Group's information security efforts

Contact information (e.g. for inquiries)

RICOH COMPANY,LTD.
Information Security Management Center
1-3-6.Nakamagome
Ohta-ku Tokyo 143-8555 Japan
Tel:03-3777-8111(Main phone number)

1 Introduction

1-1 Background and importance of initiatives in information security

In 2020, Ricoh declared an intention to transform into a digital services company. We will build an IT infrastructure for the workplace (office/worksite + home), digitalize and connect workflows, and support new ways of working. As a digital services company, we are providing optimal solutions for each customer by taking into account issues that differ from country to country, region to region, and industry to industry, and by combining Ricoh' s technological and digital capabilities. In this way, we will support the creativity of workers and change the workplace.

In the digitalized workflow, digital data of customer information is utilized in various ways to provide value, but the priority in this process is to protect the safety and security of customer information.

Unlike analog data such as paper media, digital data can easily be copied from the original. Therefore, the scope of involvement to ensure safety and security goes beyond workflow processing of digital services. It extends to the environment where the workflow is implemented, the worksite environment where products and services are manufactured and developed, the supply chain including procurement of parts necessary for manufacturing, related companies, industries, regions, and even nations.

And it is further expanding due to the increasing sophistication and complexity of services.

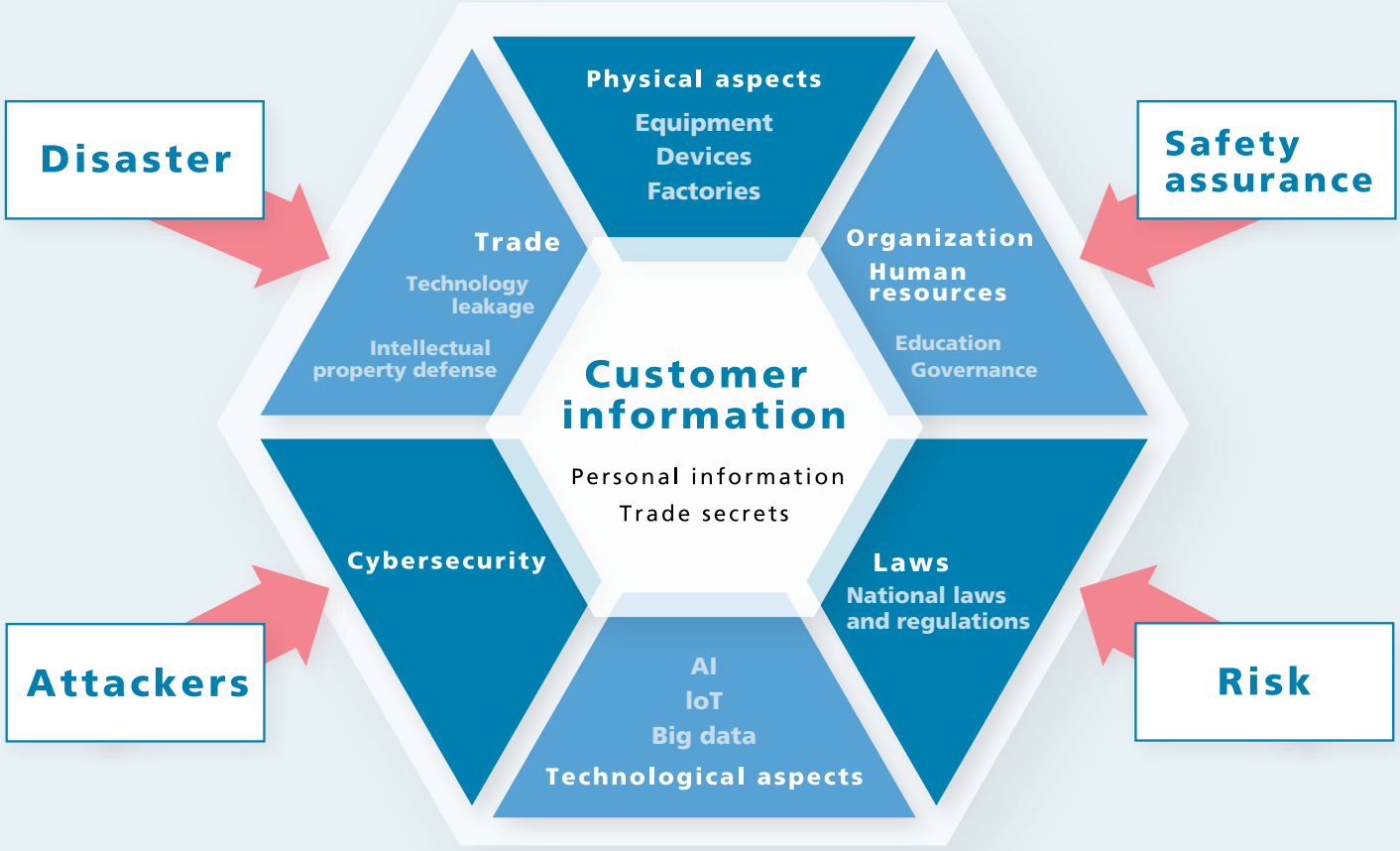
There is no end to the onslaught of malicious attackers using ransomware, malware, and the like. As shown by international security standard activities, it is important to maintain a certain level of security not only by a single company, but also through cooperation on a national level. To this end, it is necessary to coordinate efforts not only in cybersecurity, as seen in the attacks of and defense against attackers, but also in the fields of personal information protection, national laws and regulations, trade, and the like.

Ricoh regards "information security" as the scope of activities necessary to "safely and securely protect customer information from threats" and implements various measures.

This report introduces Ricoh's information security.

What is customer information?

This refers to information collected by Ricoh' s products and services, such as customer personal information, confidential customer information, information on the operation of products installed in the customer's environment, and customer inquiry information.



1 Introduction

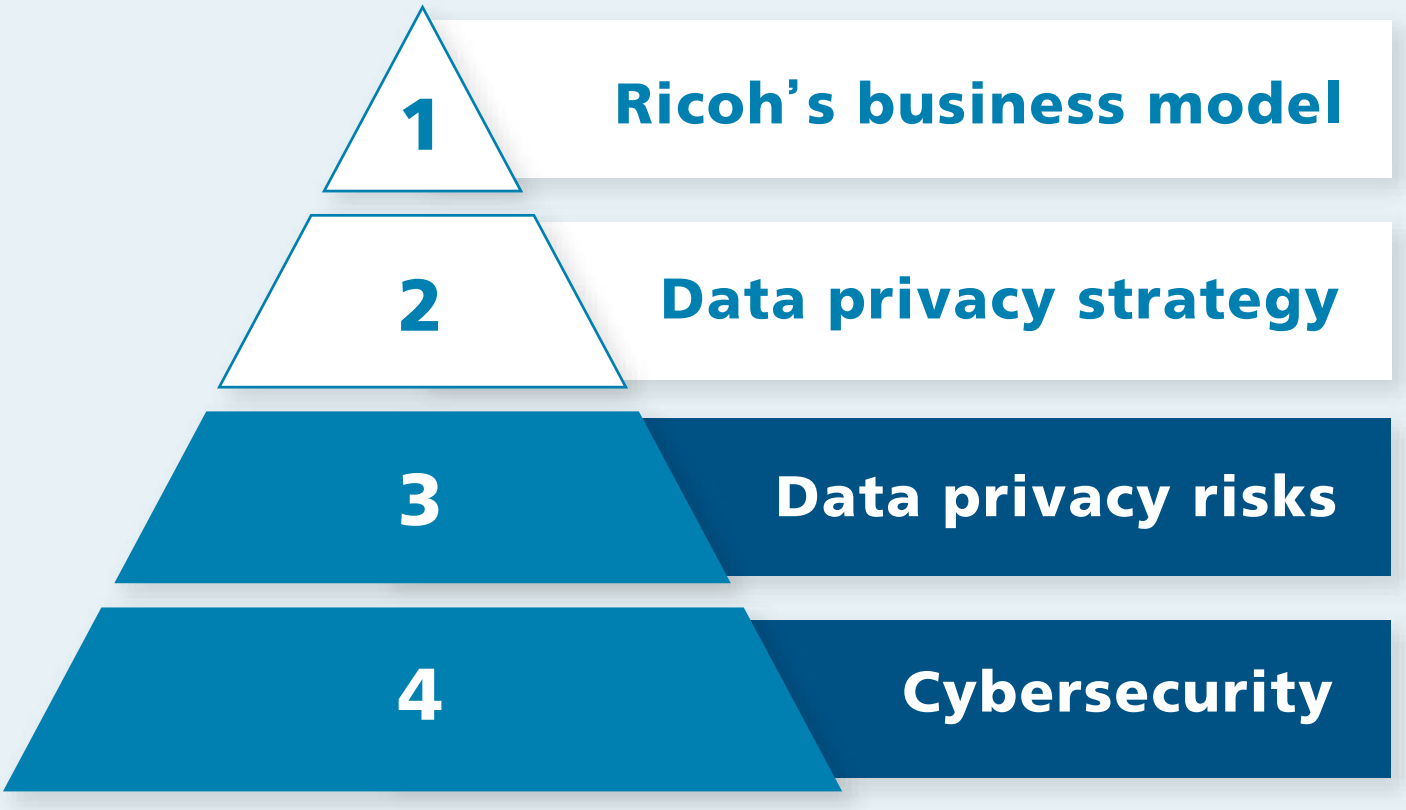
1-2 Positioning of information security in management

The Group Management Committee (GMC) and the Risk Management Committee of the Ricoh Group Executive Committee determine, in light of our management philosophy and business objectives, "priority management risks" based on a comprehensive identification of risks that may have a significant impact on management, including the impact on stakeholders, and they are actively involved in activities to address these risks.

The Ricoh Group has positioned the study and promotion of appropriate measures for the Group, which has global bases of operations, as one of the most important management issues in "priority management risks," based on constantly identifying the ever-changing information security situation, as information security measures are required at the national and international levels.

Material issues are identified based on trends in the international community, the Sustainable Development Goals (SDGs), stakeholder expectations, Ricoh' s management philosophy, our medium-term management plan, and the opinions of outside experts, and those are reviewed on a regular basis. We have identified seven material issues in the two areas of "resolving social issues through business" and "robust management foundation" to support that, and have set 17 environmental, social, and corporate governance (ESG) targets linked to each material issue. In one of the goals, stakeholder engagement, we work to strengthen security based on international security standards.

Ricoh' s information security is positioned as a necessary activity to support our diverse digital service activities such as workflow and data privacy (3, 4) and to implement value creation processes (1, 2).



2 Ricoh's information security initiatives

2-1 Concept of information security

In the Ricoh Group' s management philosophy, our mission is to "continue to create and provide new value that is useful to the world through the relationship between people and information." As a corporate citizen, we recognize that fulfilling our social responsibility is fundamental to our management, and we aim to enhance our corporate value by simultaneously creating economic value and fulfilling our social responsibility.

As a company whose business domain is linked to information fields, the Ricoh Group recognizes the importance of information security in pursuing its mission of delivering products and services that customers can use with peace of mind.

For this reason, the Ricoh Group formulated the "Ricoh Group Information Security Basic Policy" and the "Information Security Basic Policy for Products and Services" and ensures that these policies are fully known internally and externally. Additionally, we are strengthening our initiatives related to information security based on international security standards.

We regard these initiatives as activities in which all Ricoh executives and employees participate, and we promote day-to-day management and continuous improvement at worksites and on the front lines of business as well as provide customers with Ricoh products and services based on those.

2-2 Information Security Basic Policy/Individual policies

In order to improve continuously growing corporate value, the Ricoh Group has established the following policies related to information security for providing safe and secure products and services to customers and for supporting our own business infrastructure.

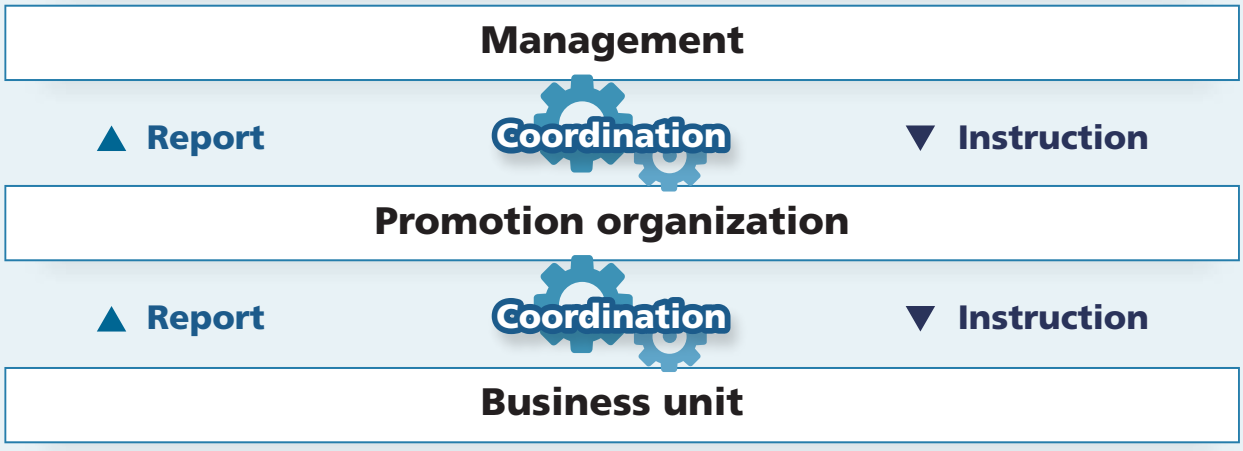
- Information Security for Products and Services
- Ricoh Group Information Security Basic Policy
- Ricoh Group Data Privacy Policy
- Ricoh Group Basic Policy for AI Technology Utilization

2-3 Security organization

In an increasingly complex and diverse business environment, the Ricoh Group considers "risk management" as being indispensable for properly managing various internal and external uncertainties related to our business and for carrying out our management strategies and business objectives.

Out of all of the risk management items, information security is positioned as a priority management risk management item, and the general manager checks the status of efforts as an evaluator. All members of the Ricoh Group, including management, promotion organizations, and business units, are working to continuously enhance information security.

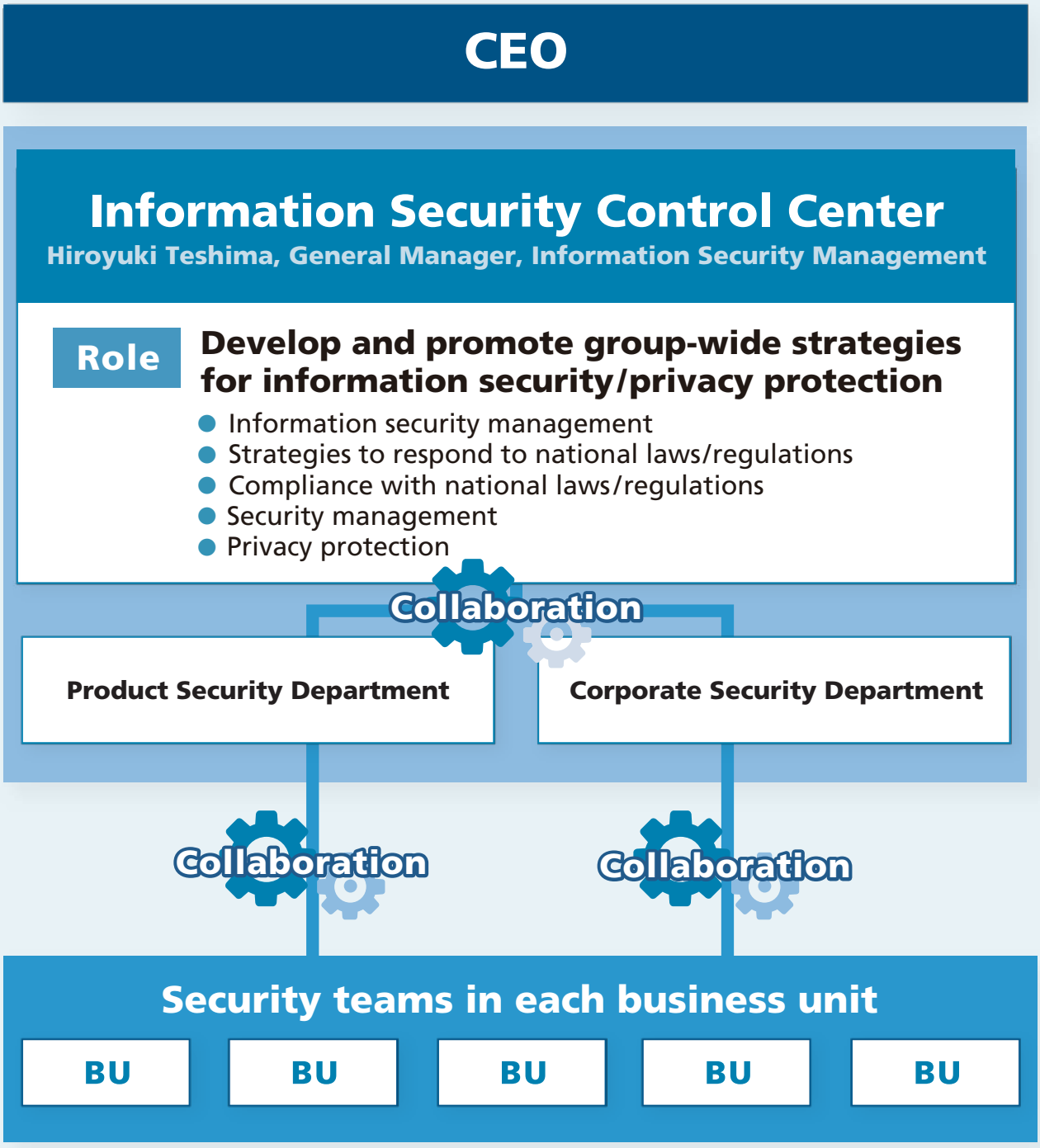
Ricoh Group's information security organization structure



2-3 Security organization

Additionally, the "Information Security Management Center" has been set up under the direct control of the CEO, and it is responsible for planning and promoting strategies for information security and privacy protection for the entire Group.

The Information Security Management Center works with Product Security Promotion Department, which is responsible for product security, the Corporate Security Promotion Department, which is responsible for information security for the entire business, and security teams organized in each business unit to strengthen Group-wide activities.



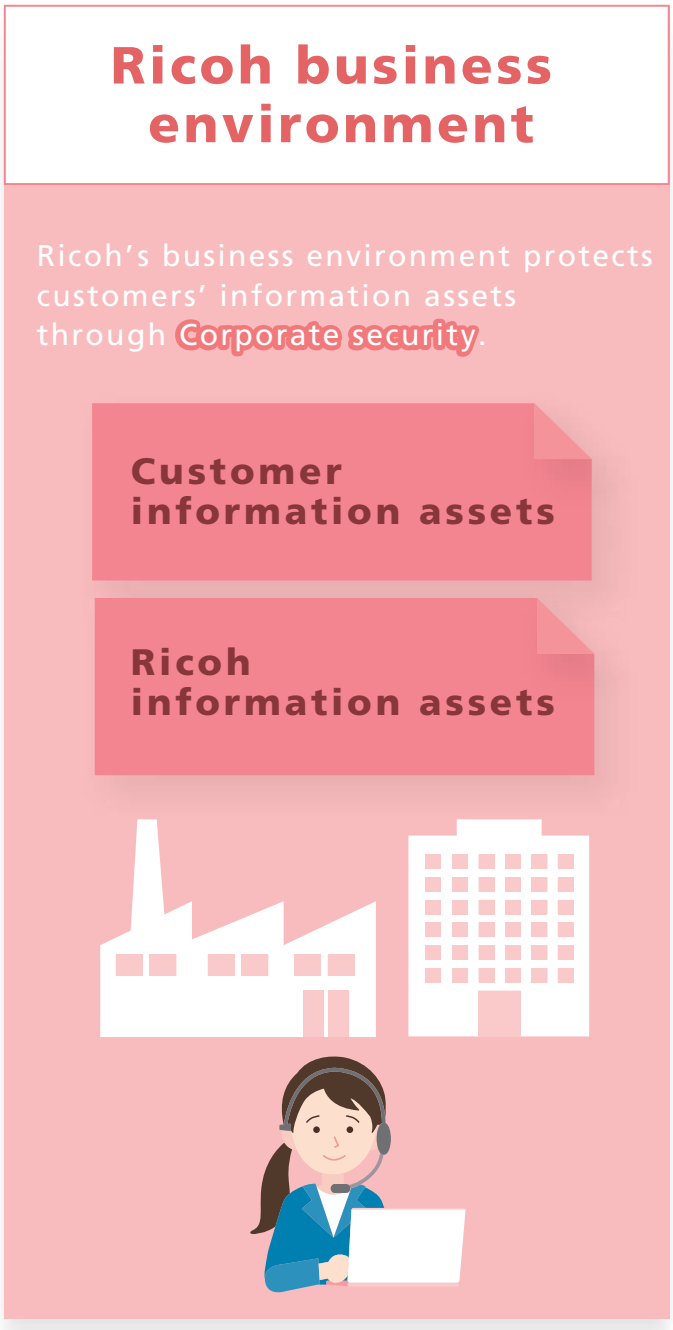
2-4 Scope of information security

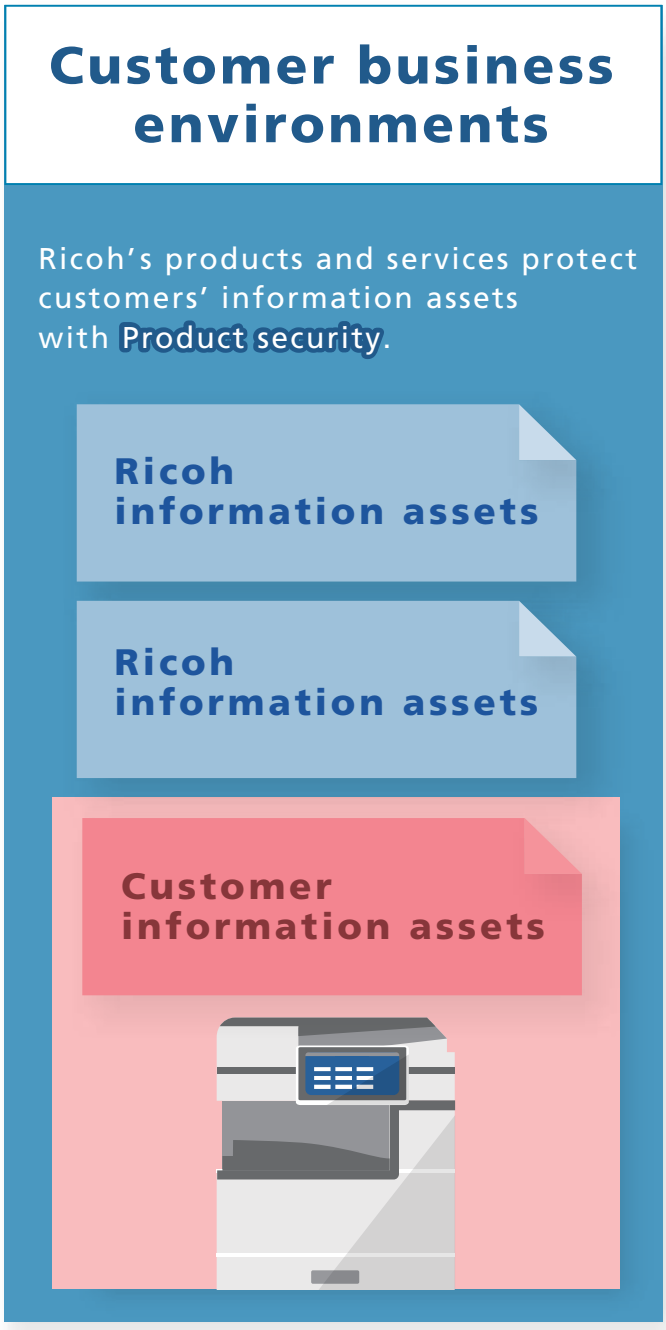
The scope covers two major areas: "products and services"and "business environment."

As described in 1-1, To ensure the safety and security of customer information we receive from our customers, not only must the products and services we provide be robust, but so too must be the business environment of Ricoh, the manufacturer that develops and produces them.

The business environment includes the value chain from product planning to sales and maintenance, information management systems used in each process, production/development/sales systems, and their operation rules/processes. In recent years, cybersecurity risks have been increasing not only from direct attacks on products and services, but also those on the business environment.

We call the activities to protect customer information handled by our products and services from attackers "product security" and the activities to protect customer information handled in our business environment from attackers "corporate security."



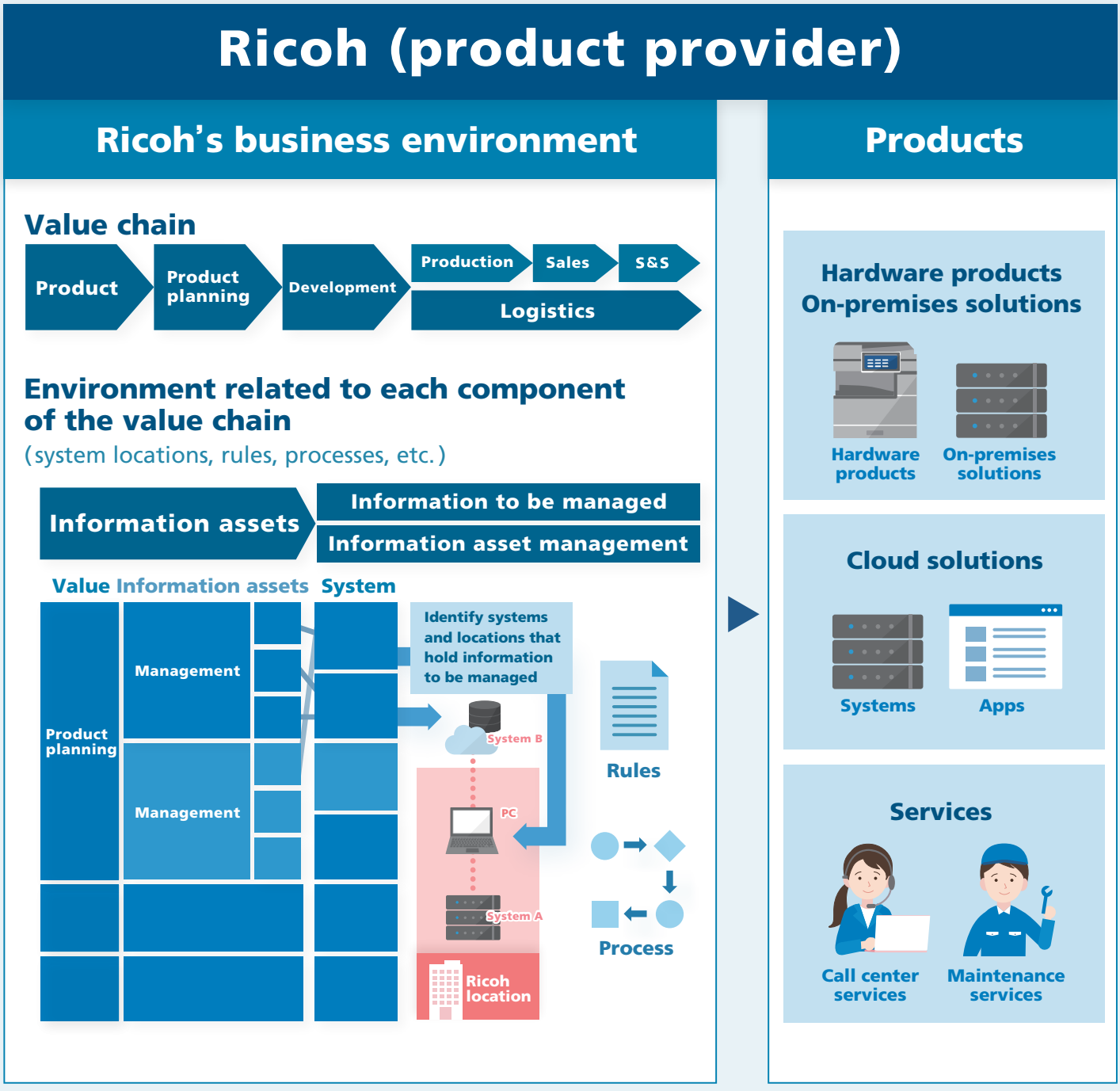


2-4 Scope of information security

Based on international information security standards (ISO/IEC*1, NIST*2, etc.), we have established and strengthened an organization that is aware of information security for the entire supply chain of our group.

We also anticipate in a timely manner security risks related to business systems in each process of planning, design, purchasing, production, sales, and we continuously study and implement countermeasures.

*1 ISO/IEC : International Organization of Standardization/International Electrotechnical Commission *2 NIST : National Institute of Standards and Technology



3 Product security

3-1 Basic policy on information security for products and services

The security policy of Ricoh Products has been established as the "Basic Policy for Information Security of Products and Services" as follows, and is It is also published on Ricoh's website.

Basic policy

The Ricoh Group provides products and services that can be used with peace of mind in keeping with the customer' s workplace and information security policies to protect the customer' s information assets and to enable the customer to make the best use of the information assets.

Basic principles

1st principle Compliance

Compliance with laws and regulations is fundamental, and this takes precedence over the second principle and the third principle.

2nd Protection of information assets

Customer information assets should be protected with each product and service and this should be given priority over the third principle on the premise that the first principle shall be satisfied.

3rd Maximize value provided

The value provided to customers by each product and service should be maximized on the premise that the first and second principle shall be satisfied. (Note: Value here is value in general of "products," and it is not limited to just that of information security.)

Action guidelines

1 Compliance

The Ricoh Group shall comply with all applicable laws and guidelines related to information security of countries where products and services are provided as well as contractual obligations.

2 Customer Origination

The Ricoh Group shall endeavor to identify the customer's needs for information security and to provide corresponding products and services.

3 Identification and Response to Environmental Change

The Ricoh Group shall endeavor to identify changes in the information security environment and to provide products and services that respond to those.

4 Response to Information Security

The Ricoh Group shall regularly analyze information security risks of products and services and strive to reduce those risks.

5 Information Security Management

The Ricoh Group shall create and continuously improve on an information security system for products and services.

6 Customer Value Maximization

The Ricoh Group shall strive to provide products and services solutions that combine convenience and safety.

January 2018

Ricoh Company, Ltd.

Representative Director, President and Chief Executive Officer

Yoshinori Yamashita

3-2 Pursuit of safe and secure products

3-2-1 Security by design

To ensure that our customers can use our products and services with peace of mind, we are committed to implementing security by design, which ensures information security from the planning and design stages.

In-house regulations based on ISO/IEC 27034-1, the international standard for secure development, have been established and are being gradually applied.

3-2 Pursuit of safe and secure products

3-2-2 Bringing attention to security risks

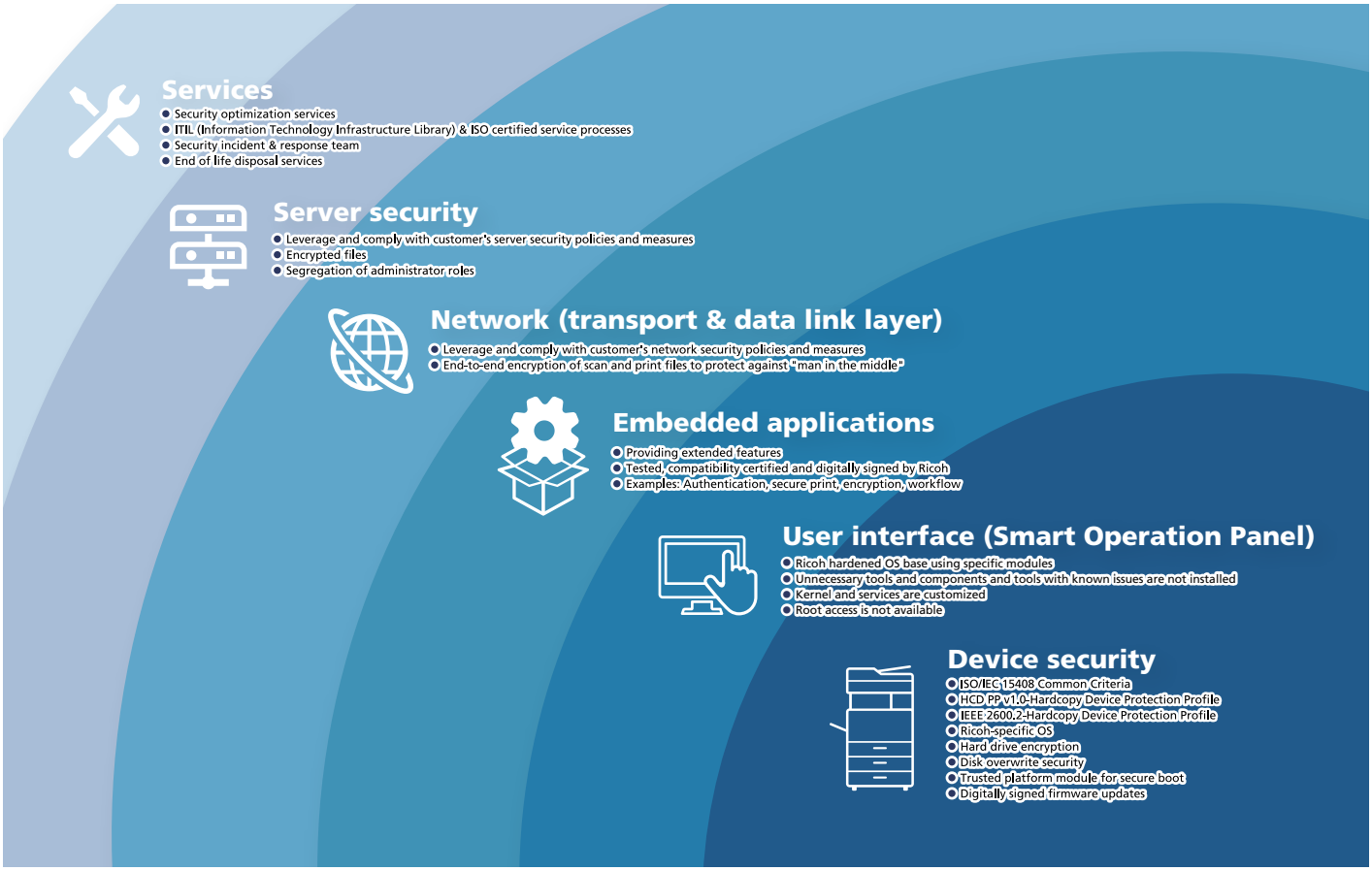
With the development of an information society, various threats such as computer viruses, leakage of personal information, and unauthorized external access are all around us. In response to increasingly diverse threats, security initiatives are being taken up as one of the most important issues for our customers.

These security threats are not limited to PCs, servers, and networks. Security threats to Ricoh products and services can also be mitigated through proper configuration and operation. To ensure the safety of our products and services, we recommend certain actions be taken.

In addition, we are working on early response to vulnerabilities based on ISO/IEC 29147/30111, an international standard for vulnerability countermeasures, such as alerting the status of response to vulnerabilities with risk of high cyber attack, establishing a contact point to receive vulnerability reports from security researchers, and providing vulnerability countermeasure information.

3-3 Ricoh's layered approach to security

In order to protect customer data from various security threats, for our products and services we always refer to the latest international security standards and follow various technological trends such as encryption, OSS vulnerability management, data authority management, and secure development processes.



4 Corporate security

The Ricoh Group established common standards in March 2007 and has been promoting the full-scale deployment and entrenchment of those common standards at our Group companies since April 2007. With these common standards, we aim to continuously improve the information security response level of each company and further bolster the foundation for providing new value to customers.

In order for the Ricoh Group to fulfill our corporate social responsibility and enhance our corporate value through information security initiatives, it is important for us to make security levels be common so as to raise the information security of each company above a certain level, transcending the boundaries between group companies.

Even within the same corporate group, there are many differences in size and corporate culture of the individual companies, and each company has a wide range of operations, which may include research, development, design, production, sales, and service. There also tend to be differences in the level of information security addressed on an individual basis.

The Ricoh Group has recognized the need for common standards that would serve as a unified security policy for the entire Group in order to resolve these various problems and make the Group Information Security Management System (ISMS), which serves as the foundation for information security activities, even more effective.

Additionally, the ISO/IEC 27001 international standard does not specify the extent to which individual safety measures should be implemented, so specific implementation standards were necessary. In response to the requirements of the international standard, we began studying standards for implementing information security according to the degree of risk in December 2005, established the Ricoh Family Group Information Security Measures (RFG ISMeasures) in March 2007, and have been promoting the full-scale deployment and adoption of those at our Group companies since April 2007.

For more information, visit
https://www.ricoh.com/security/management/activity/standard.html

In addition, cyber attack tactics have become increasingly complex and sophisticated in recent years, making it difficult to respond to such attacks with just an ISMS approach that focuses on "prevention."

In response to this situation, we have adopted the concept of the Cyber Security Framework (CSF) issued by the National Institute of Standards and Technology (NIST) in the USA, which focuses on "early detection and rapid response" assuming attack or intrusion, and the "OODA" method, which is highly responsive to ever-changing attacks, in order to conduct cybersecurity response.

4 Corporate security

4-1 Ricoh's corporate security strategy

As ransomware and other cyber attacks targeting companies become more complex and sophisticated, Ricoh is promoting strategic and global cybersecurity measures.

Security Strategies

Countermeasure status visualization and planning
(NIST CSF compliance, risk-based planning)

In response to cyber attacks such as ransomware and other threats that have been making headlines in recent years, it is no longer sufficient to simply comply with the previous ISMS requirements for information security measures (hereinafter referred to as the "requirements"), which focus on "prevention."

Against this background, we also refer to the requirements of the Cyber Security Framework (CSF) to improve cybersecurity measures, visualize the status of response to security threats using heat maps, and develop and implement risk-based plans for assessment and security enhancement.

Adoption of OODA

In ISMS activities, the PDCA (plan-do-check-act) cycle was used to improve the level of security.

The PDCA cycle is a good method for implementing activities to achieve clear objectives. But it is not suitable for dealing with events such as cyber attacks, where there are many external factors beyond our control.

By also using the OODA (observe–orient–decide–act) cycle, a method that is highly responsive to events such as ever-changing cyber attacks, we are strengthening our security management system by dividing activities to achieve objectives (PDCA) and activities to respond to changing circumstances (OODA) as appropriate.

Perspectives of information security measures

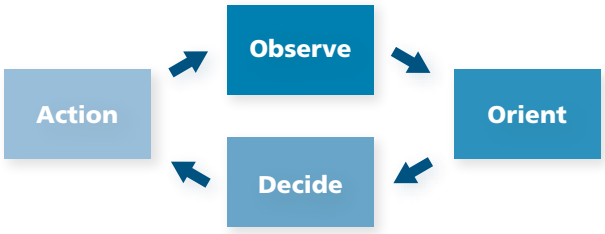
Identification and defense (ISMS activities)

In order to protect the organization's important information assets, we will improve the level of information security measures by continuing this cycle of identifying the situation inside and outside the organization, prioritizing the resolution of identified issues, and formulating and implementing plans to resolve issues.

Detection, response, and recovery (cyber attack response activities)

In the area of cyber attacks, SOC ※1 / CSIRT ※2 organizations are set up in each region globally, and those perform timely monitoring and judgment of the situation and take prompt actions / responses based on appropriate decisions to minimize the impact.

※1 **SOC** : Security Operation Center
※2 **CSIRT** : Computer Security Incident Response Team



In cyber attack response activities, one of our operations, we are required to respond to ever-changing attack situations. Therefore, we adopt "OODA" (observe–orient–decide–act), a method that excels in immediate response.

4 Corporate security

4-1 Ricoh's corporate security strategy

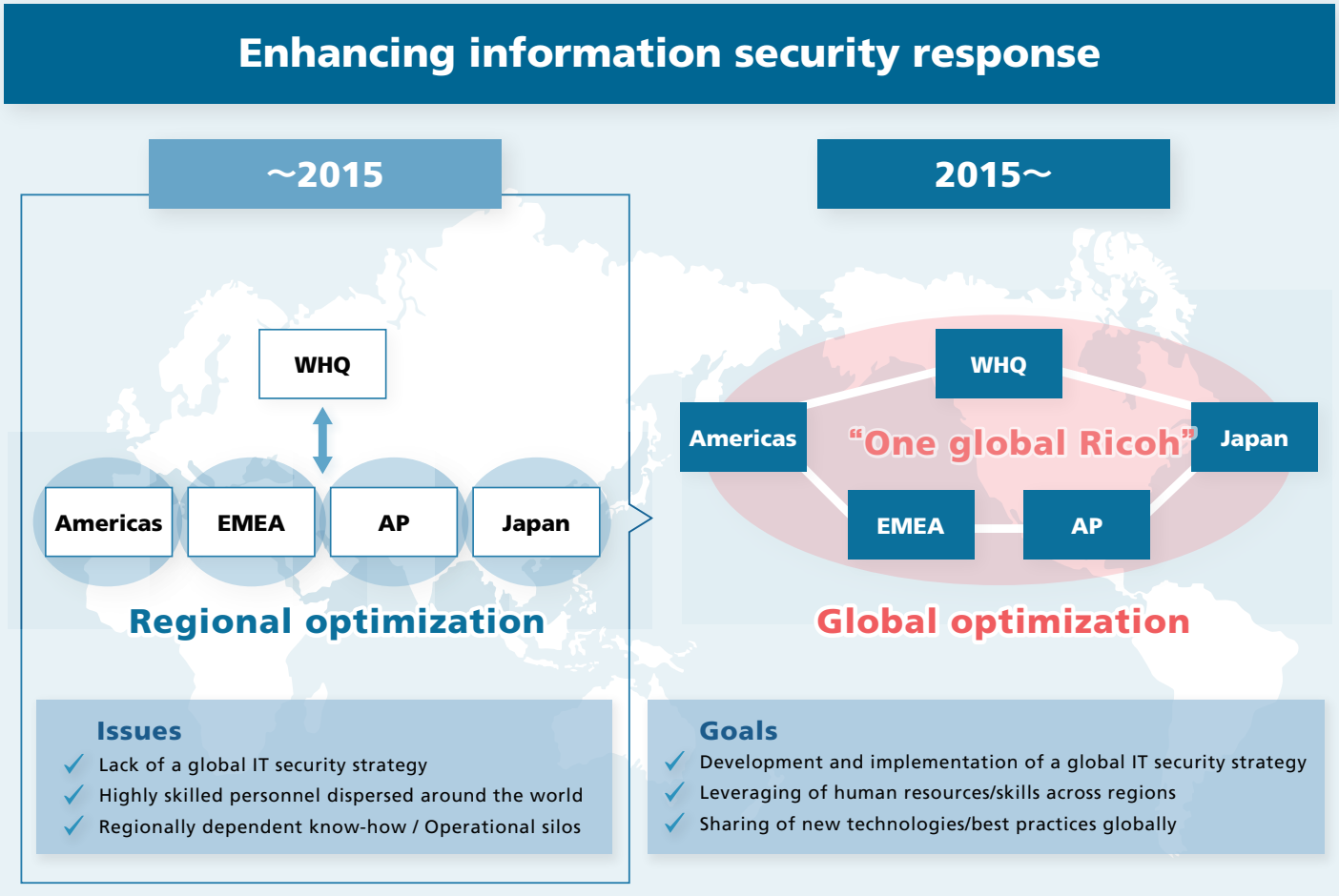
Global response

As Ricoh is expanding business globally, we believe that our security measures require response that is consistent on a global scale. Ricoh organized VOIT (Virtual One IT) in 2015 to improve the homogeneity of security strength globally and to accelerate coordination among security personnel.

Aims of VOIT

- Promote a global information security and risk management program
- Establish Group information security policies, standards, and procedures
- Improve security awareness at the regional and global levels
- Review security implementation plans across the globe
- Share information on identified vulnerabilities and support mutual response

VOIT organization structure



4-2 Enhancing security incident response

We have established a Computer Security Incident Response Team/Security Operation Center (CSIRT/SOC) structure and are working constantly to strengthen that to enable us to respond promptly to cyber attacks, which have become more prevalent.

Establishment and Operation of CSIRT

The RICOH-CSIRT was organized in FY2013 to analyze threats based on incident reports from the SOC, information from external CSIRT organizations, and information from security information websites.

The team also leads the rapid and optimal response (evidence preservation, attack analysis, root cause investigation, prevention of spread, and containment) to the identified threats.

Establishment and Operation of SOC

A Security Operation Center (SOC) has been organized to constantly monitor IT systems owned by the Ricoh Group and conduct detailed analysis of suspicious events.

This enables early detection of incidents by quickly detecting unauthorized intrusions from outside and unauthorized use from inside, and it also enables linking with response teams as necessary.

Use of outside security experts

With cyber attacks becoming more sophisticated and complex, it is difficult to complete all security response in-house.

Therefore, Ricoh has introduced a Managed Security Service (MSS) by partnering with security experts, and are collaborating with various security organizations to always utilize the most advanced security technologies.

4-3 Security training

In order to protect information assets from threats, it is essential to establish and disseminate rules and implement systems as well as to ensure that each employee has a high level of security awareness and skills. Ricoh conducts security training and awareness programs regularly in order to develop human resources knowledgeable about that.

Security training

We are promoting training to raise awareness of issues related to security risks that one must be aware of in day-to-day work, such as precautions to be taken while traveling and working remotely, how to use cloud services, and anti-virus measures, and to understand the correct way to respond to such risks so that we can work in a secure manner.

Targeted e-mail attack training

In addition to familiarizing employees with how to recognize and respond to fraudulent e-mails suspected of being cyber attacks, we have them experience receiving and responding to emails simulating cyber attacks in order to deter damage from actual attack e-mails.

Desktop training on incident response

In response to the threat of cyber attacks, it is important not only to prevent damage from occurring, but also to prevent the spread of damage and to recover quickly if damage should occur.

For this reason, we regularly conduct simulated cyber attack drills.

Security communication

In cybersecurity, it is important not only for employees to have basic knowledge, but also to keep up with the latest trends.

To this end, we regularly send and share information on security trends and internal security responses to such trends in the form of “security communication” for employees throughout the company.

5 Data privacy

Against the backdrop of the rapid progress of digitalization and the utilization of big data, concern about data privacy and the protection of personal information* is growing daily on a global scale. Compliance with the General Data Protection Regulation (GDPR) and other national laws and regulations on data privacy is a priority issue for companies to maintain competitiveness.

Since the enactment of the Act on the Protection of Personal Information in Japan in 2005, revised laws have been enacted due to technological advancement and changes in social conditions such as globalization of business.

Ricoh has been transforming into a digital services company, and in 2021, we launched data business in earnest with the release of the "AI at Work" series, a new service that uses proprietary natural language processing AI (artificial intelligence) and other technologies to support business operations.

Meanwhile, the rules for the use of personal data are still not clear, and it is difficult for companies to determine to what extent use of personal data is appropriate for them.
Furthermore, from the customer' s point of view, uncertainty about whether their personal data is being handled appropriately and whether their privacy is being properly protected are causes for concern.

For this reason, Ricoh has defined a data privacy policy for all personal data, including customer personal information to ensure compliance with all laws and regulations regarding customer information.

5-1 Protection of personal information

At the Ricoh Group, we recognize the utility of personal information (including personal numbers and specified personal information) in the global information society and the importance of protecting the rights and interests of individuals, and we comply with relevant laws, regulations and other rules to ensure that all personal information handled in the course of business is used appropriately and effectively.

Since the enactment of Japan's Act on the Protection of Personal Information in 2005, the Ricoh Group has established, operated, and managed our own regulations in consideration of international trends in the protection of personal information, and we have made sure these regulations are known by all employees and other relevant personnel. Moreover, we are continuously maintaining and improving our regulations and are complying with the revised Act, which took effect in April 2022.

* Personal information is information that can be used to identify an individual.
* Personal data is the name given to all information about an individual, whether or not the individual can be identified.

5-2 The Ricoh Group's Data Privacy Policy

The Ricoh Group's vision of a sustainable society is expressed as the "Three Ps Balance", in other words, a society that maintains a balance among the three Ps of Prosperity (economic activities), People (society), and Planet (environment).

In order to realize the society the Ricoh Group aims to achieve, we strive to solve social issues and contribute to society.

1 Basic Policy for Personal Information

In accordance with the Ricoh Group' s Basic Policy for Personal Information Protection, we comply with all relevant laws, regulations, and other rules to protect privacy.

Companies within the Ricoh Group may also operate under additional privacy policies appropriate for their operations and develop products and services in accordance with such policies.

2 Privacy and Security

The Ricoh Group will handle customer information appropriately in accordance with our Basic Policy for Personal Information Protection and will apply appropriate measures to protect customers.

In addition, we will strive to promote the confidentiality, integrity and availability of collected customer information in accordance with the Ricoh Group Information Security Basic Policy and the Ricoh Group Information Security Basic Regulations for Products and Services.

3 Information handled by the Ricoh Group

The Ricoh Group will handle customer information for the purposes of providing products and services to our customers, improving the quality of our products and services, and considering development of new products and services.

4 Transparency and accountability

The Ricoh Group will strive to ensure the appropriate use of customer information and provide explanations based on the intended use and situation.

5-3 The Ricoh Group's Basic Policy for AI Technology Utilization

The Ricoh Group' s mission is to provide excellence to improve the quality of living and to drive sustainability based on the Spirit of Three Loves—a dedication to people, one' s country, and a passion for work—that constituted the principles of Ricoh founder Kiyoshi Ichimura.

In line with this mission, the Ricoh Group has established the following policy to provide fulfillment to people, efficiency, and convenience through integrating and leveraging advanced technology and AI we have accumulated.

1 Respect for Human Rights

The Ricoh Group will apply AI based on our Human Rights Policy.

2 Data Privacy Policy

The Ricoh Group will handle customer information based on the Ricoh Group Data Privacy Policy.

3 Fairness

We recognize that the use of AI may introduce bias in the results. Therefore, we will strive to avoid bias in our use and application of AI.

4 Creating New Value

The Ricoh Group will create new value by using AI, while working closely with customers and earning their trust, to help them grow and solve their problems.

Aiming to establish a security brand

The growing need for information protection due to the increasing number of cyber attacks worldwide is now becoming universal and common knowledge.

The constant struggle against attackers is likely to continue and not slow in the future.

The Ricoh Group will continue to strengthen and improve our efforts in information security to ensure that we can respond flexibly as a digital services company. We will do that while keeping a close eye on changes in the external environment, such as the strengthening of security standards across industries and countries. And we will continue to strengthen our information security organization in order to achieve that goal.

RICOH
imagine. change.

RICOH COMPANY,LTD.
1-3-6.Nakamagome
Ohta-ku Tokyo 143-8555 Japan

https://www.ricoh.com/

● Contact us