Advancing with you
MS&AD
INSURANCE GROUP

# Research of SMB's Cybersecurity measures in Japan 2021

MS&AD InterRisk Research & Consulting

# Introduction

Accidents and damage caused by Cybersecurity incidents are on an increasing trend year by year, and it is very common to see these reports on media. Information security is a management subject and, taking information security measures is an important issue that can no longer be avoided as enterprise and SMB's management.

Therefore, this time, we surveyed the actual condition of enterprises and SMBs aimed at contributing to the reduction of information security risk in the future.

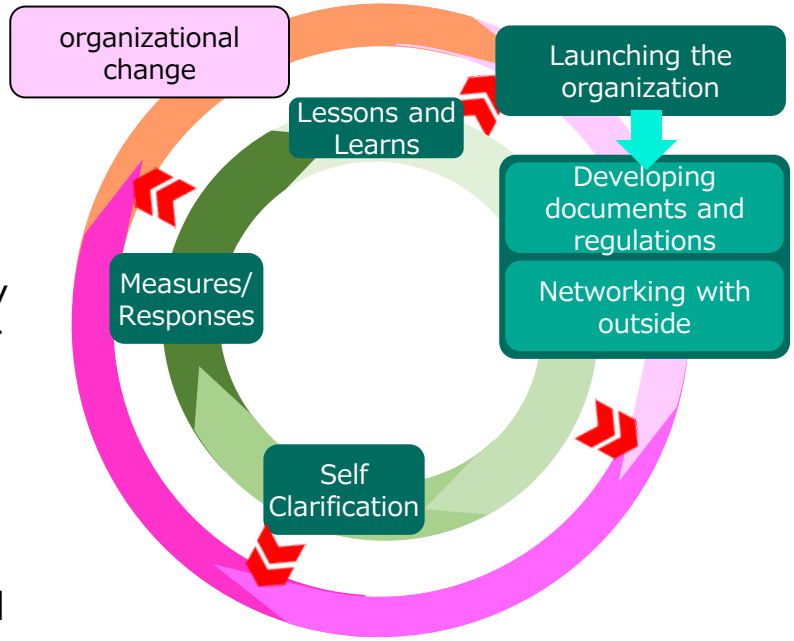
We hope this survey will be helpful to companies for further efforts.

# Findings and Recommendations

The following is a summary of the findings of the survey and recommendations based on them.

## ① Improving cybersecurity organization will lead to organizational change.

Companies that have a Cyber Security organizational structure have relatively superior results in cybersecurity measures. It is thought that the establishment of Cyber Security organizational structure will help to clarify the measures to be taken by the company by initiating improvement activities, and by having the newly established structure belong to an organization outside the company and incorporate external information.
In addition, it was found that the effect of organizational structure development is not limited to the cybersecurity field, but also works to the advantage of promoting telework and cloud utilization. It is believed that security measures can encourage the incorporation of new technologies and corporate reforms.




## ② Achieving a sustainable supply chain by improving organizational structure

Companies with organizational structures in place are more likely to have cyber countermeasure requirements across the supply chain than companies without organizational structures in place. We believe that the establishment of an organizational structure will lead to entry into the supply chain, improvement in corporate value, and stability.

### ③ Recommendation to improve system and enhance security through "Managed Security Services

The survey revealed a trend that security equipment such as network monitoring is not being operated as installed, and that companies without an organizational structure are not considering the introduction of endpoint security EDRs. The Managed Security Service is an operational service for security equipment that provides both monitoring by security experts and security enhancement. This service is particularly useful for companies that do not have an organizational structure or the time to develop one.

### ④ Consider the need for insurance, including additional services.

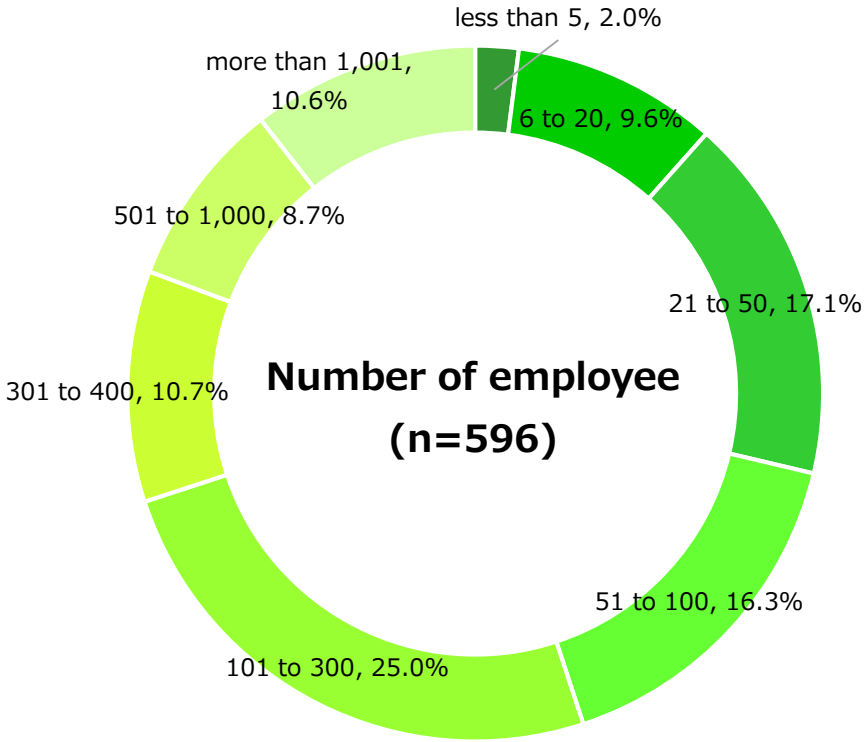
While cyber insurance subscription rates remain low, the survey found that awareness of cyber insurance itself is gradually increasing. The survey also found that companies that do not have cyber insurance are seeking ancillary services that function during response and initial response. Cyber insurance not only compensates for damages caused by accidents, but also has emerged as a service that reduces the risk of accidents occurring and damage spreading, and it is hoped that this service will be utilized.

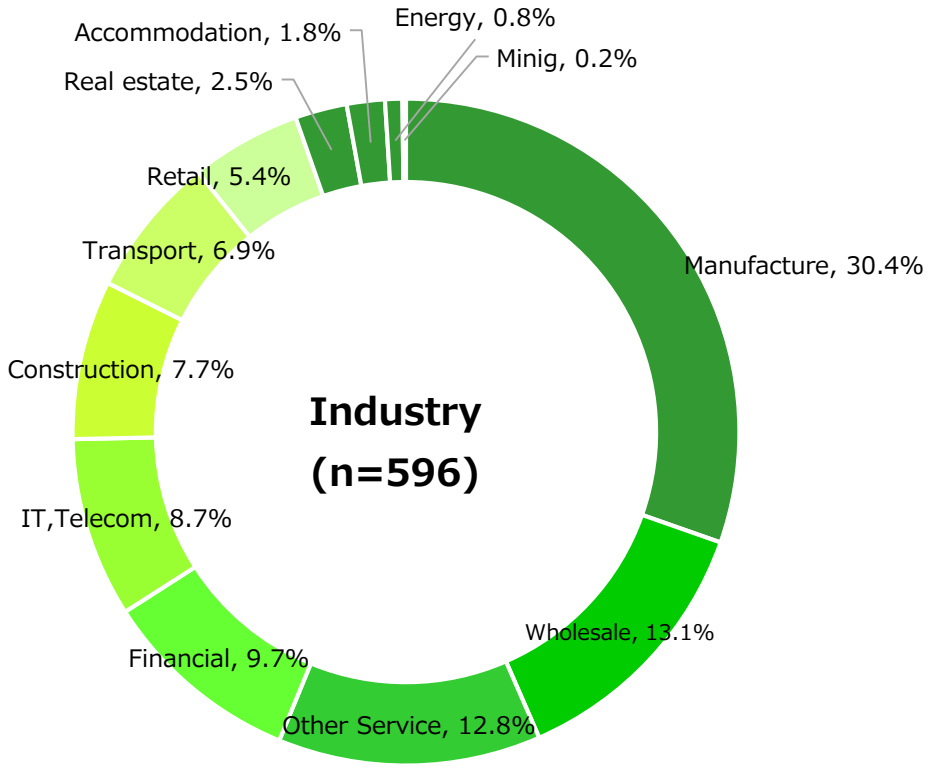
# Overview of the Research

# Overview of the Research

| | |
|---|---|
| Survey method | Mailing questionnaire (combined with Web response) |
| Targeted companies | 10,000 companies in Japan<br>Extracted from Toyo Keizai Inc.'s "40,000 company data in Japan ((1) Basic data)"<br>Companies that randomly extracted in industry by industry |
| Number of valid responses | 596(total collected number: 600)<br>Recovery rate 5.9% |
| Survey period | November 18, 2021 - December 4, 2021 |
| Analysis Method | Simple and cross tabulations<br>*Percentages were rounded to one decimal place, so individual percentage totals may not add up to 100%.<br>*The number of "non-responses" was not included in the population. |

# Industry and size of the companies



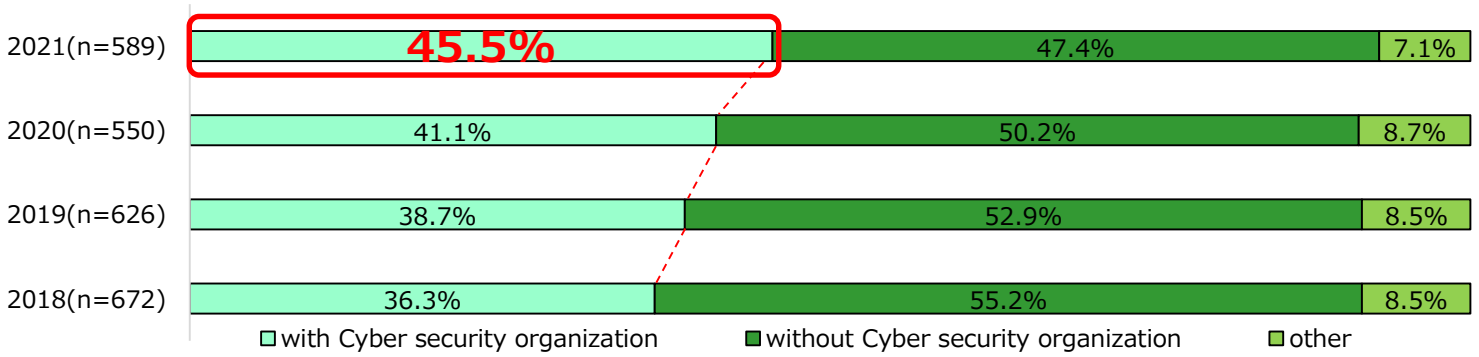



# Internal Organization Management

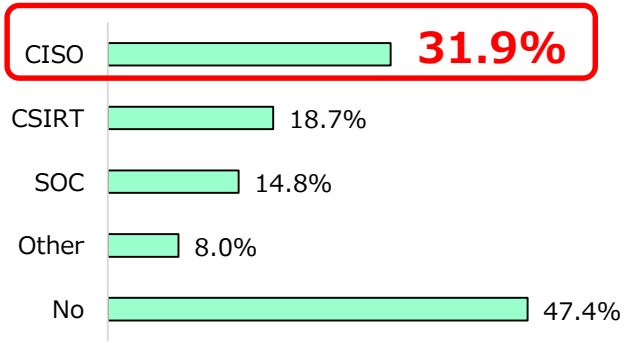
Advancing with you
MS&AD
INSURANCE GROUP

# cyber security organizational structure * Multiple selection (1/2)

Companies with a Cyber Security organizational structure was 45.5 %, which was less than half of the respondents, but the percentage is increasing year by year.
" CISO " ( 31.9 %) was the most popular in the companies that replied "Yes".



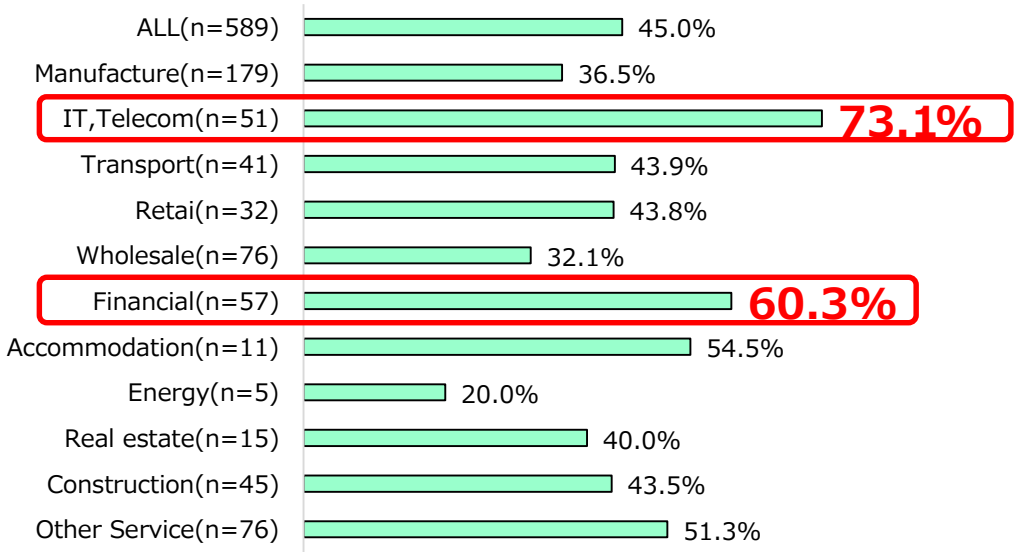

| | |
|---|---|
| CISO | Chief Information Security Officer<br>( Also known as : Information Security Officer, Information Security Chief, Chief Information Security Officer, etc.)<br>A position that supervises the information security of an organization.<br>Its main roles are to formulate a security policy (action guideline), direct measures to be taken when a security incident occurs, bridge information security-related matters to management, and manage information security within the organization. |
| CSIRT | Computer Security Incident Response Team<br>An organization that responds to incidents (accidents) and events related to cyber security, such as information leaks and system failures caused by cyber attacks. Conduct research and other activities during normal times other than when an incident occurs (emergency). |
| SOC | Security Operation Center<br>An organization that monitors and analyzes logs generated by information security devices, servers, computer networks, etc., and detects and notifies cyber attacks. There are cases of monitoring within the own organization and service-providing SOCs that monitor customers. |



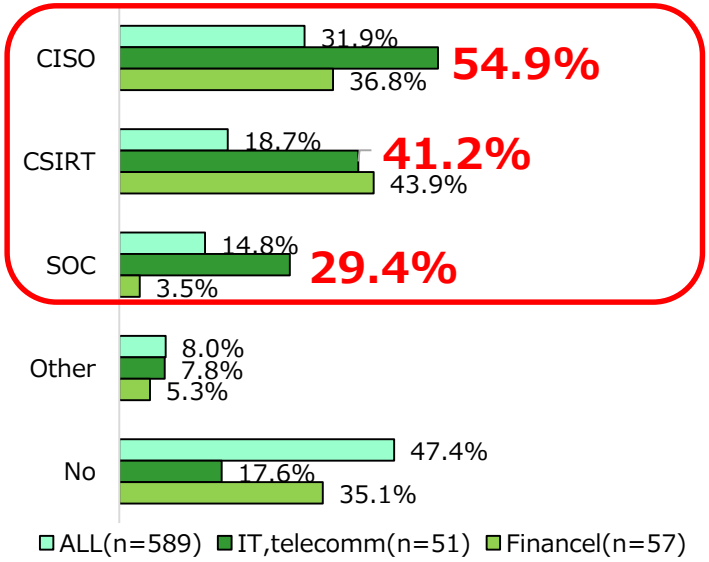
# cyber security organizational structure * Multiple selection (2/2)

The industry with the highest percentage of companies that answered that they have a information and telecommunications industry ( 73.1 %) was followed by the finance and insurance industry ( 60.3 %) .
information and telecommunications industry, the ratio of building SOCs in addition to CISOs and CSIRTs is larger than the total.
reasons for not building a system are “There are no the human resources and budget " and " The management is not aware of cyber security issues. "

**With organization （by industry)**

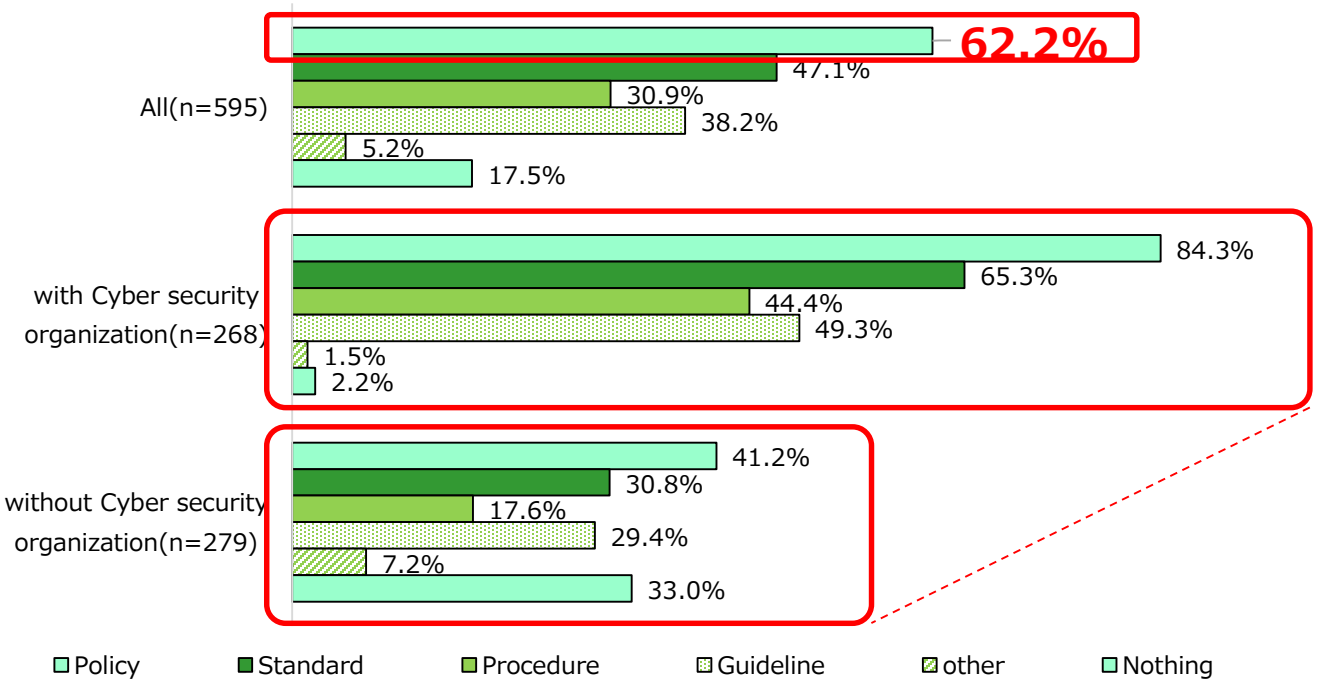



**cyber security organizational structure**
(ALL、IT/Telecomm、Financail)



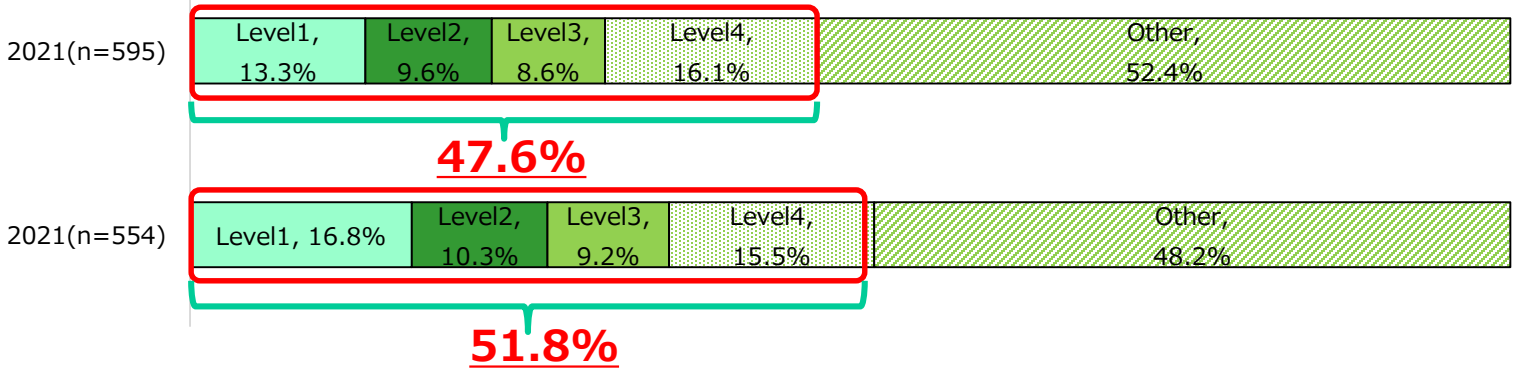
# Documents for cybersecurity *Multiple selection (1/2)

The most frequently established security-related document/regulation was the **"policy (policy/action guideline)" (62.2%).**In addition, companies that have a cyber security organizational structure are more likely to have well-developed documents and rules, according to the results of the survey.
The reasons given by companies that chose "No" for not having security-related documents/rules included "Do not feel the need" and "It is an implicit rule".



# Documents for cybersecurity *Multiple selection (2/2)

The status of maintenance of security-related documents and regulations was classified into five categories by level as shown below, assuming that they are maintained in the following order: policy => standard => procedure => guideline. This year, only 47.6% of companies maintained documents and rules in order, slightly lower than the previous year.

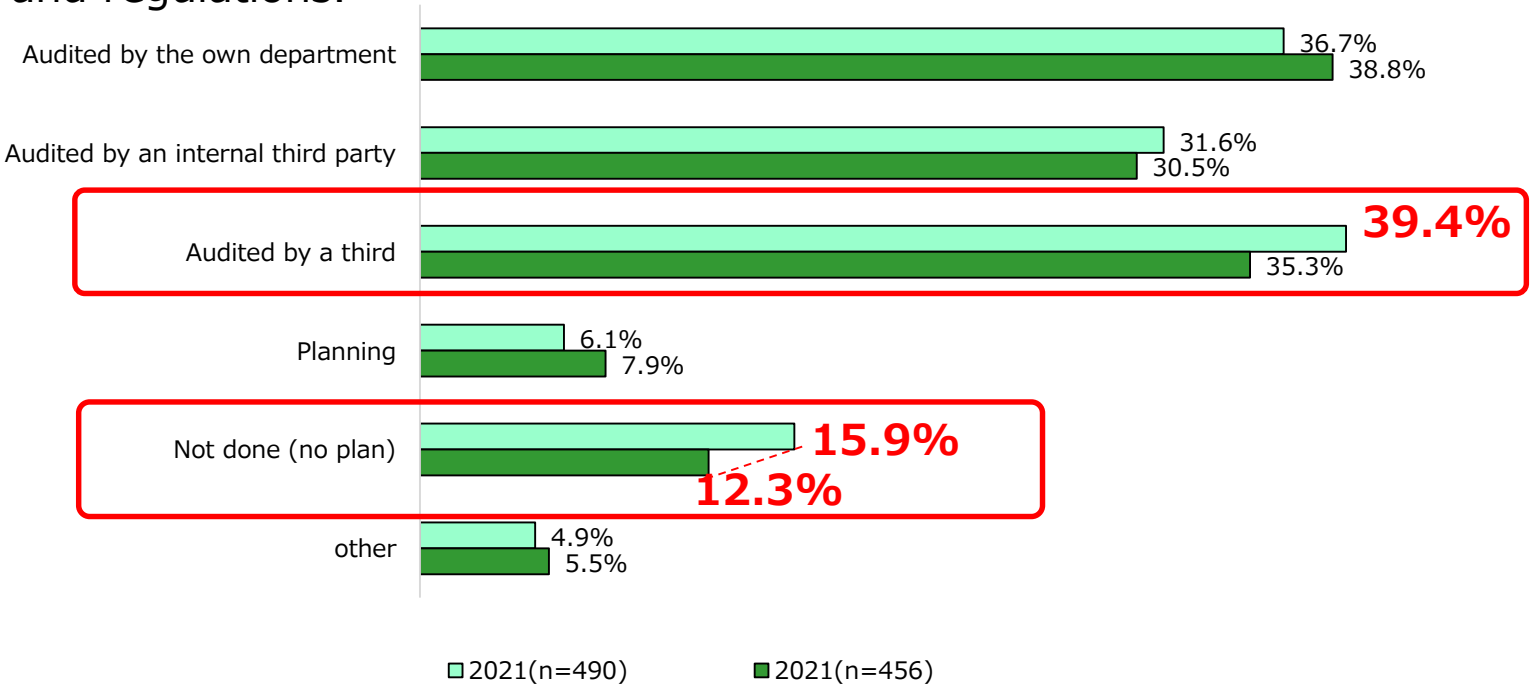



| | Policy | Standard | Procedure | Guideline |
|---|---|---|---|---|
| Level 4 | ○ | ○ | ○ | ○ |
| Level 3 | ○ | ○ | ○ | — |
| Level 2 | ○ | ○ | — | — |
| Level 1 | ○ | — | — | — |
| Other | Items that do not fall under Levels 1-4 | | | |

# Audit of the documents *Multiple selection

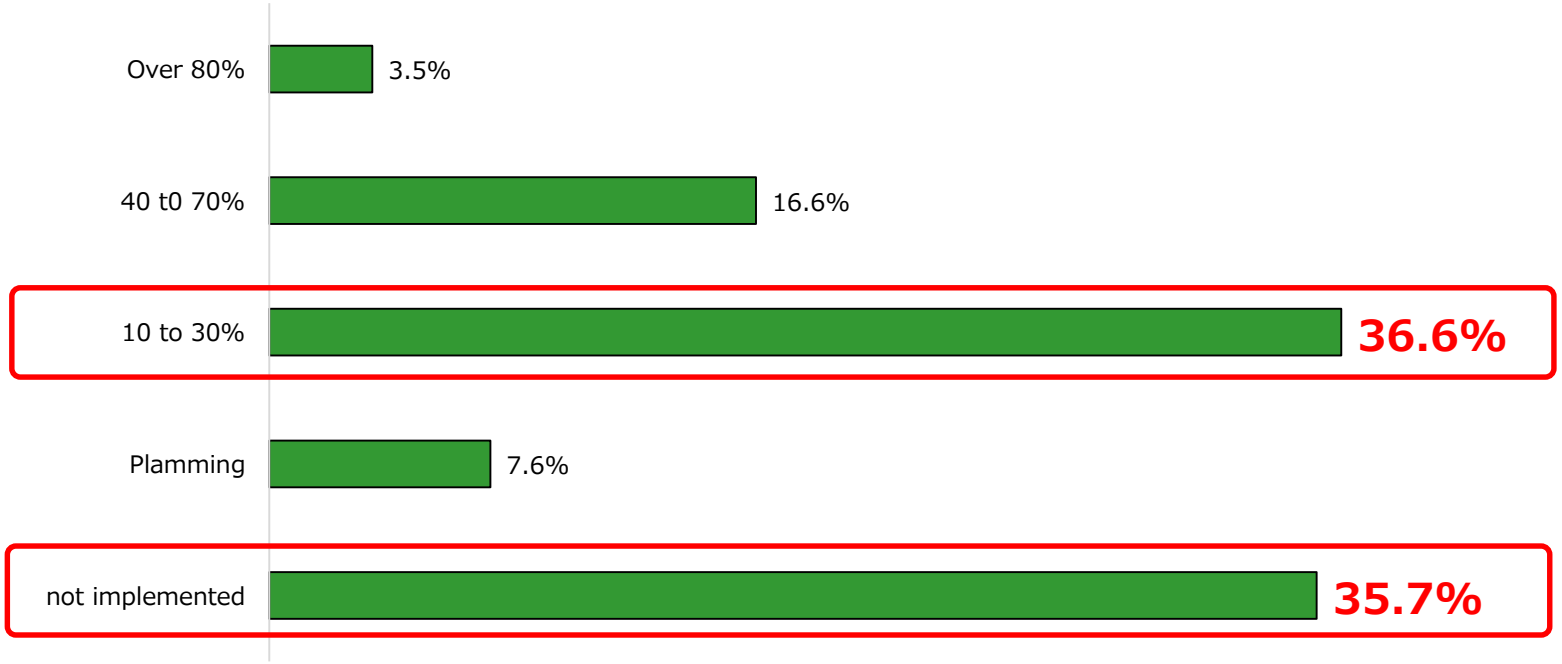
(When they answered that they have documents in the previous question)

Among the companies that answered that they have documents and regulations, we asked whether they are checking and auditing whether the contents described in the security-related documents and regulations are being implemented. The most common answer was "Audited by a third" (39.4%). Compared to the previous year's survey, "Not done (no plan)" was slightly higher, indicating that the system has not made much progress along with the aforementioned maintenance of documents and regulations.



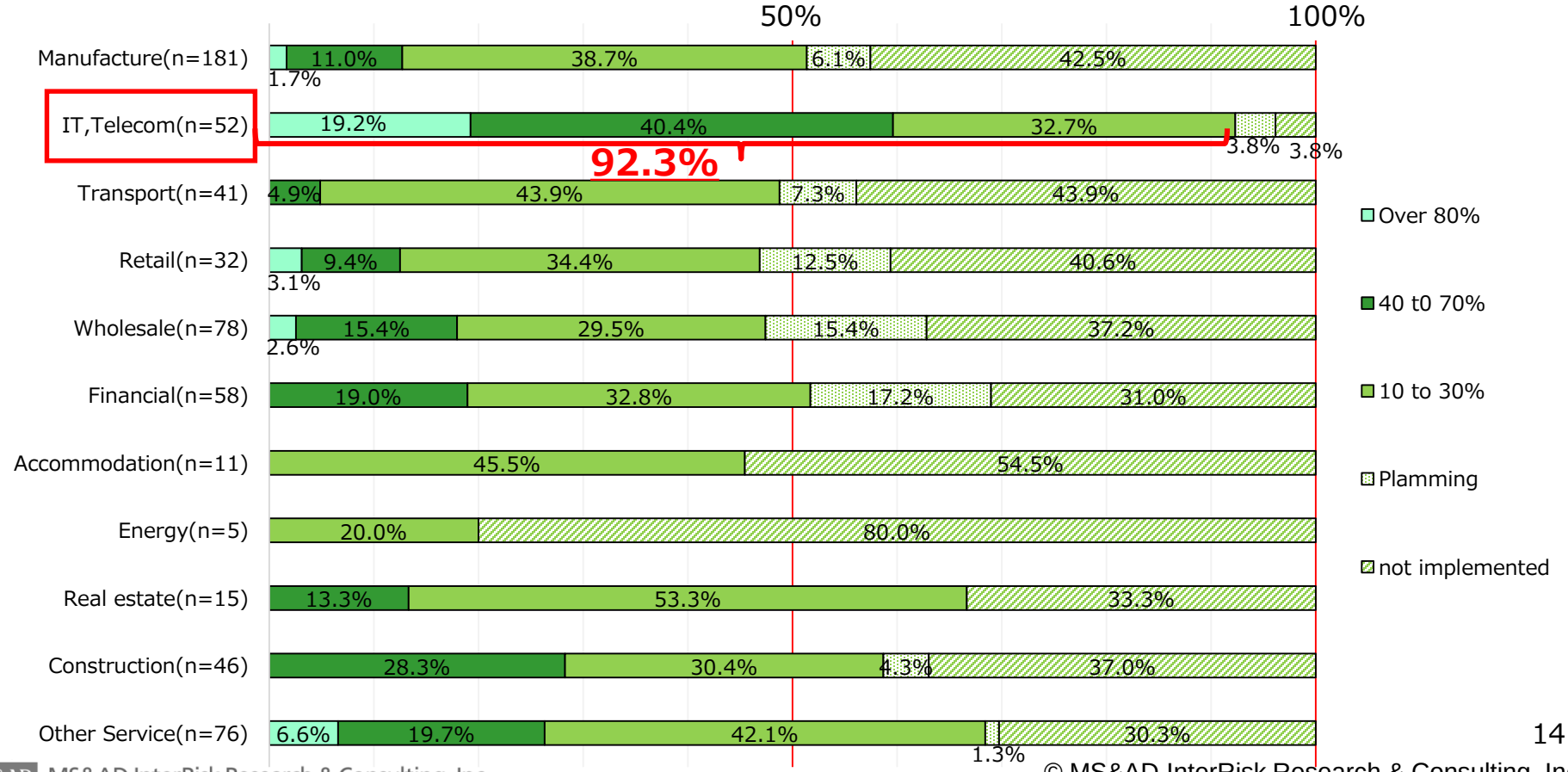
# Percentage of telework operations(1/3)

When asked about the "percentage of operations that can be conducted through telework when the number of all operations is 10," the most common response was "10 to 30%" (36.6%), followed by "not implemented" (35.7%).



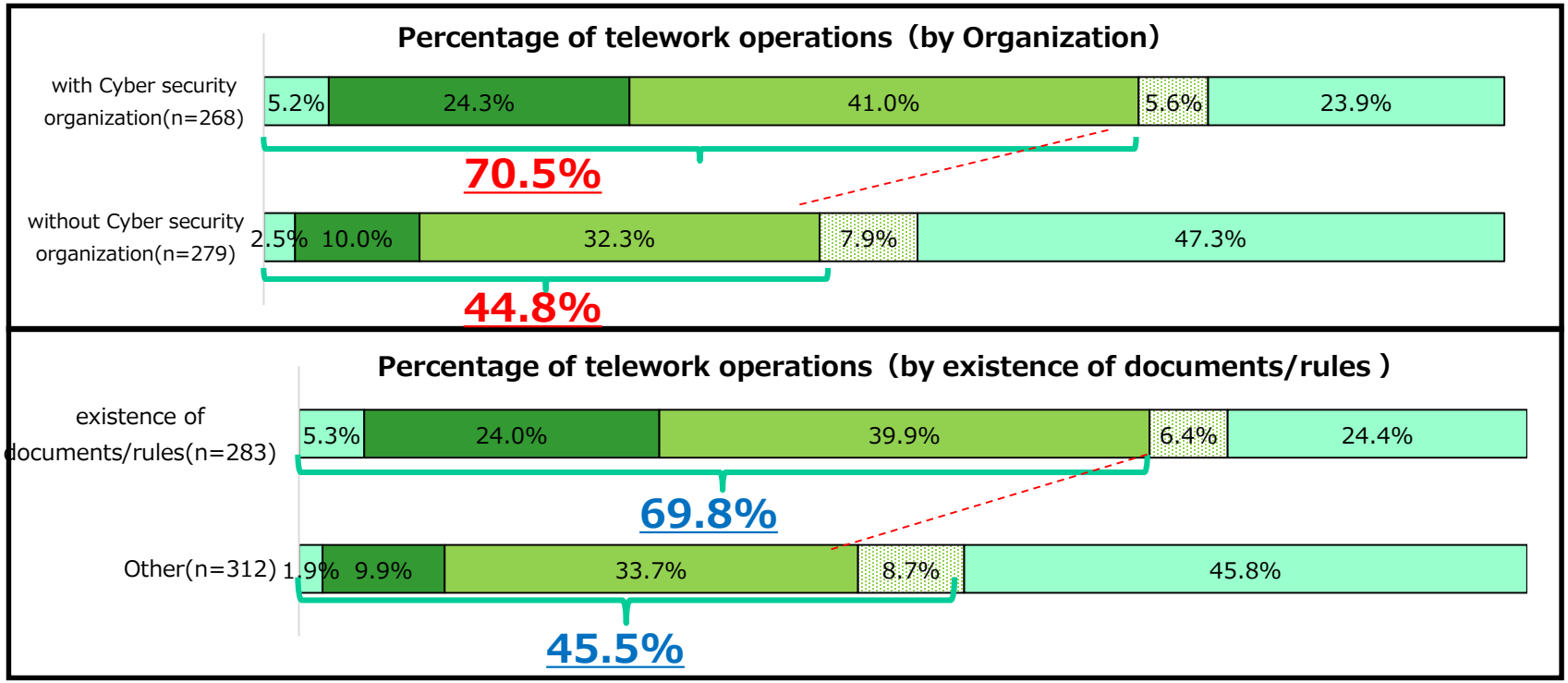
# Percentage of telework operations(2/3)

It was found that teleworking is more advanced in the information and telecommunications industry than in other industries. **The information and telecommunications industry has an advantage, including the aforementioned cybersecurity system development status.**



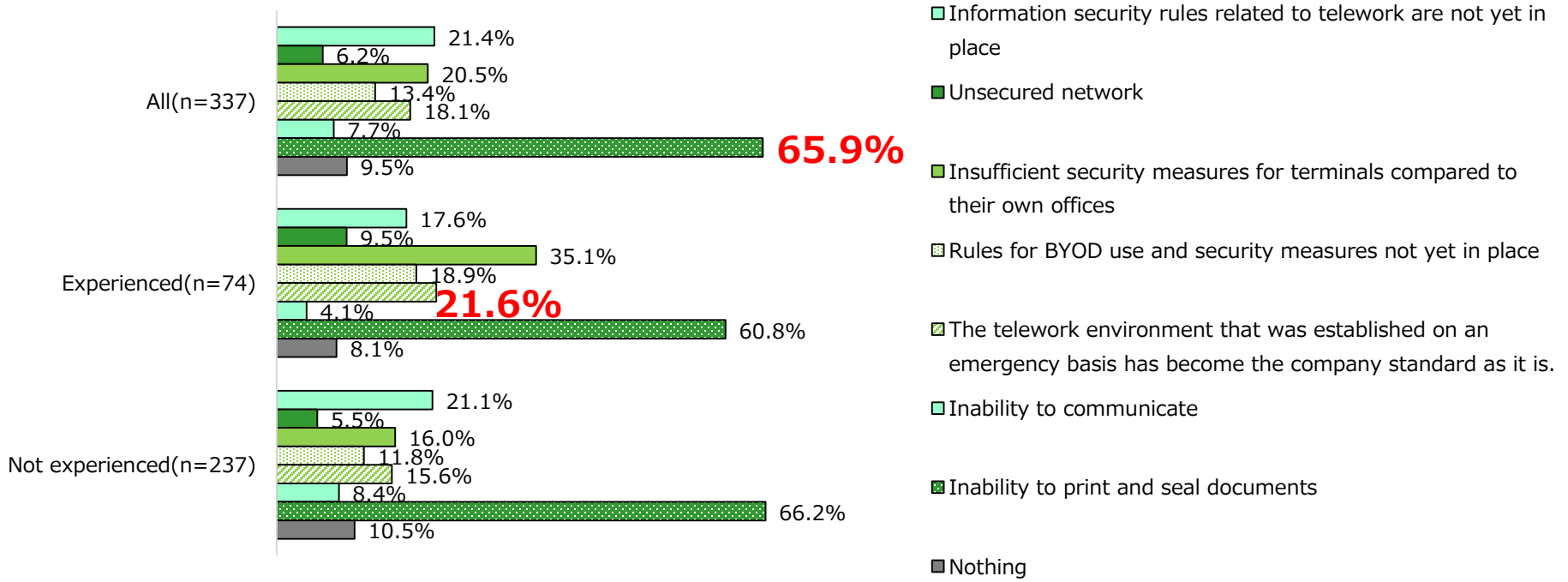
# Percentage of telework operations(3/3)

Furthermore, the results by cyber security organizational structure and by existence of documents/rules showed that the companies that answered "Yes" to each question had a higher percentage of operations conducted through teleworking.It is considered that the development of a telework system together with the development of a cyber security system and rules will lead to the promotion of telework.



# the issues in implementing telework *Multiple selection

When asked about the issues in implementing telework, the most common answer overall was **"Inability to print and seal documents" (65.9%).**When asked if they had experienced a cyber incident, companies that had experienced a cyber incident recognized "Insufficient security measures for terminals compared to their own offices" (21.6%) as an issue.

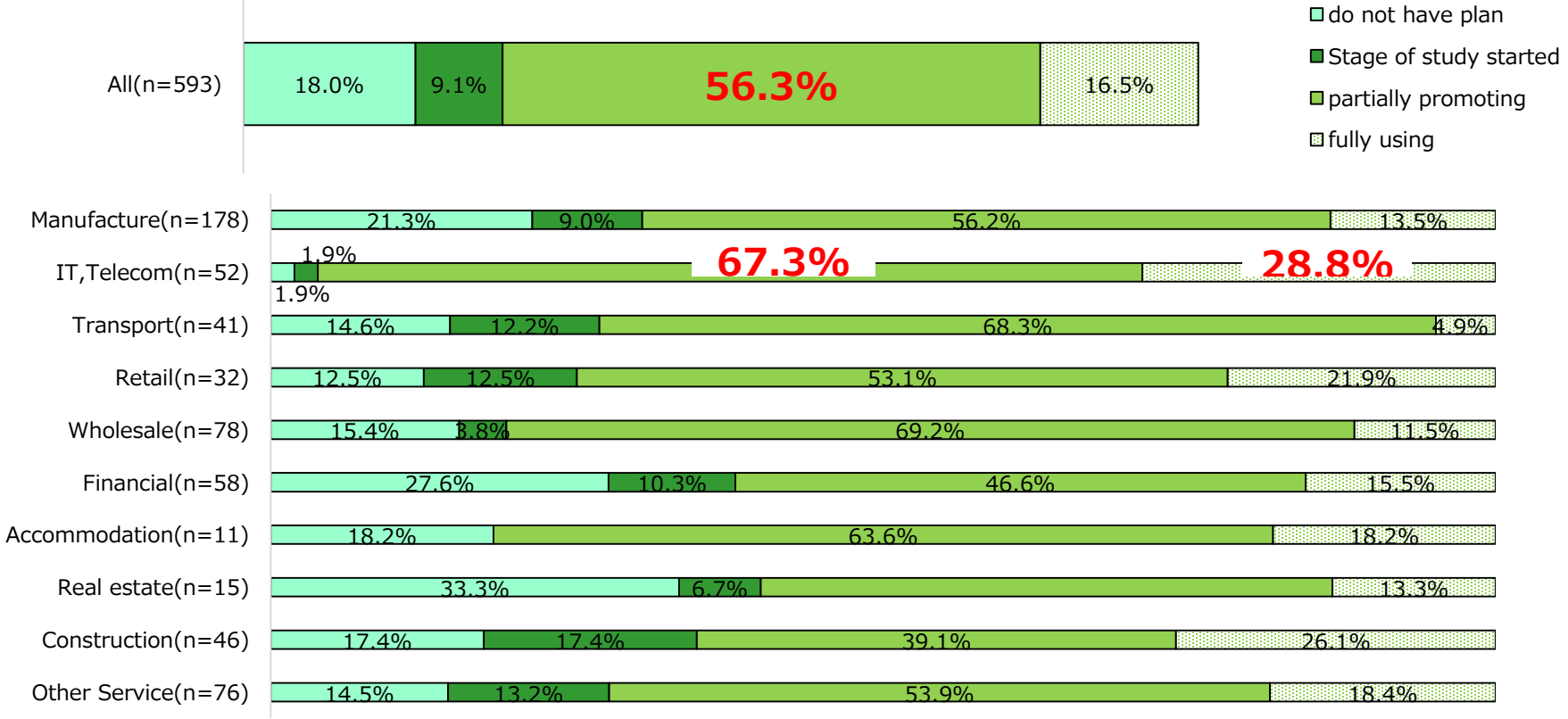


# 3rd Party (Subcontractor) Management

Advancing with you
MS&AD
INSURANCE GROUP

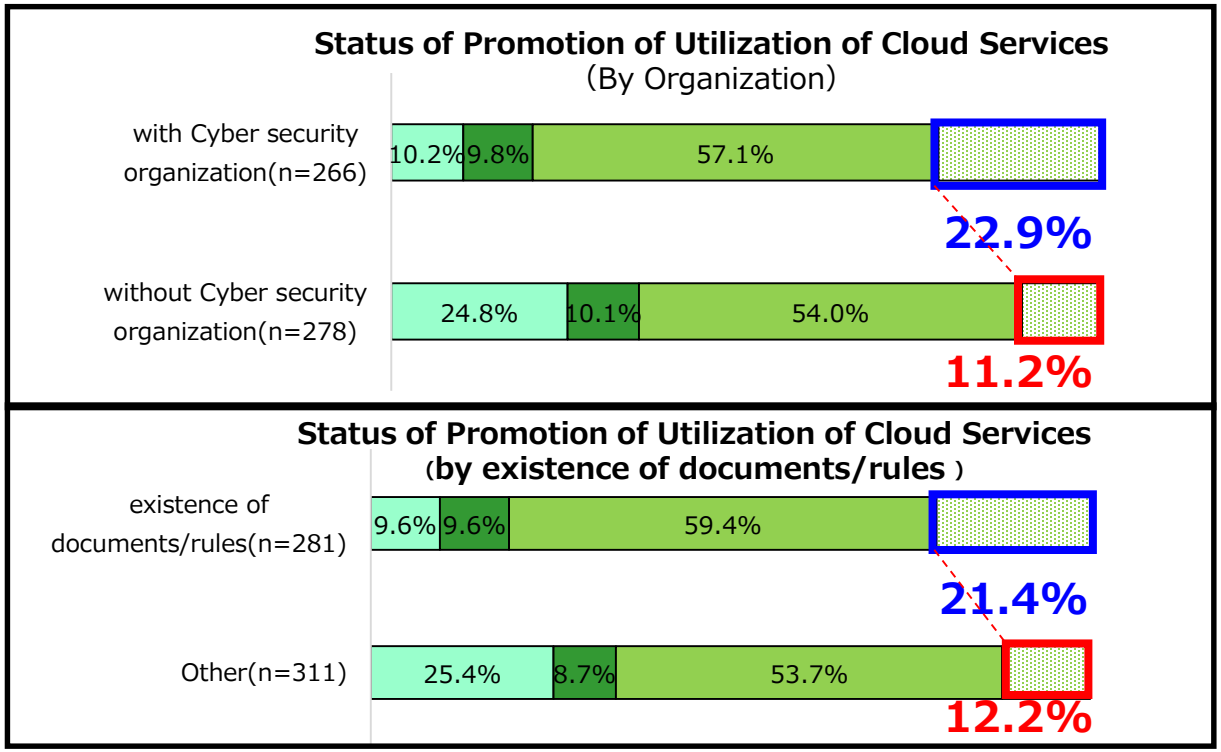
# Status of Promotion of Utilization of Cloud Services(1/2)

This year, we started a survey on the status of promotion of cloud service utilization.The most common answer overall was **"partially promoting" (56.3%)**.By industry, the information and telecommunications industry had the highest percentage of respondents who answered that they were **"fully using" (28.8%) and "partially promoting" (67.3%).**



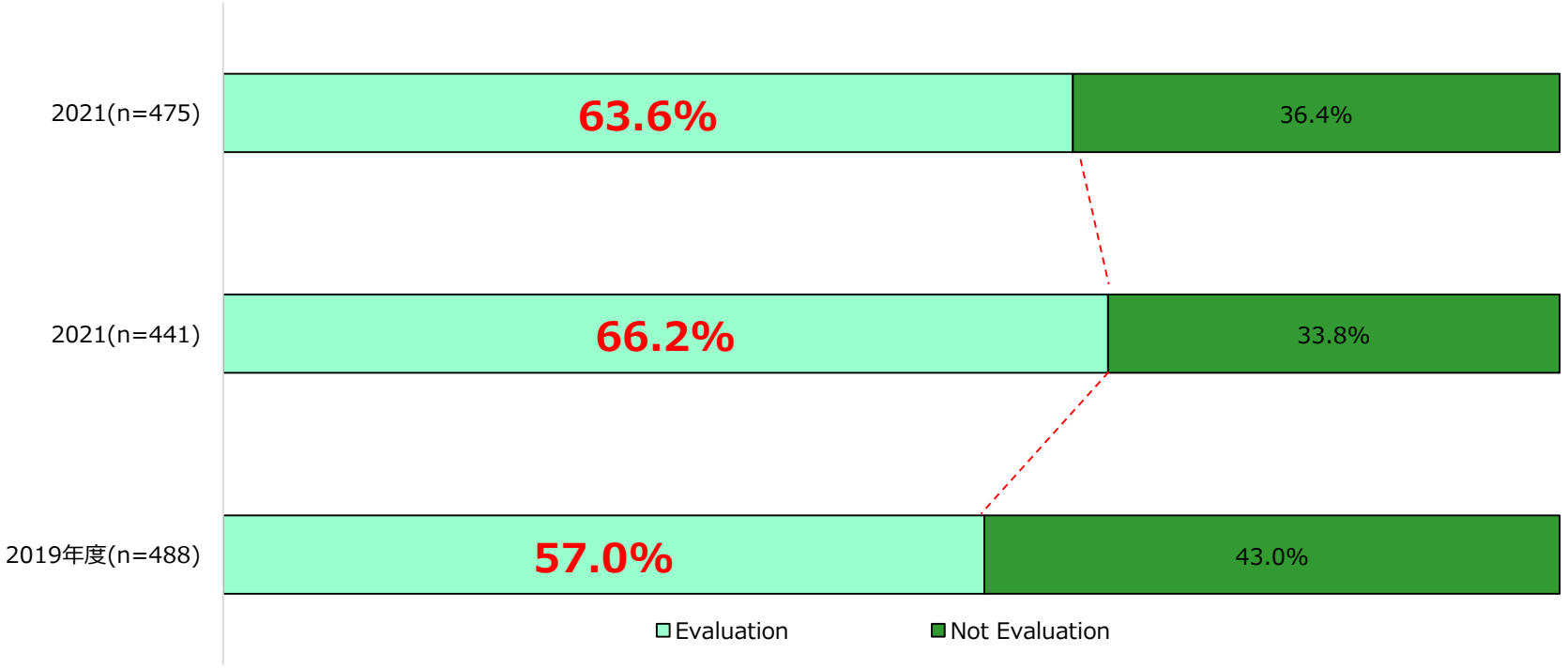
# Status of Promotion of Utilization of Cloud Services(2/2)

In addition, the results by cyber security organizational structure and documents/rules showed that companies that answered "Yes" to each question were more likely to promote the use of cloud services, especially those that answered "fully promoting" were **twice** as likely as those that answered "Yes". **the key to promoting the use of cloud services is to implement them together with the development of a cyber security organizational structure and rules.**



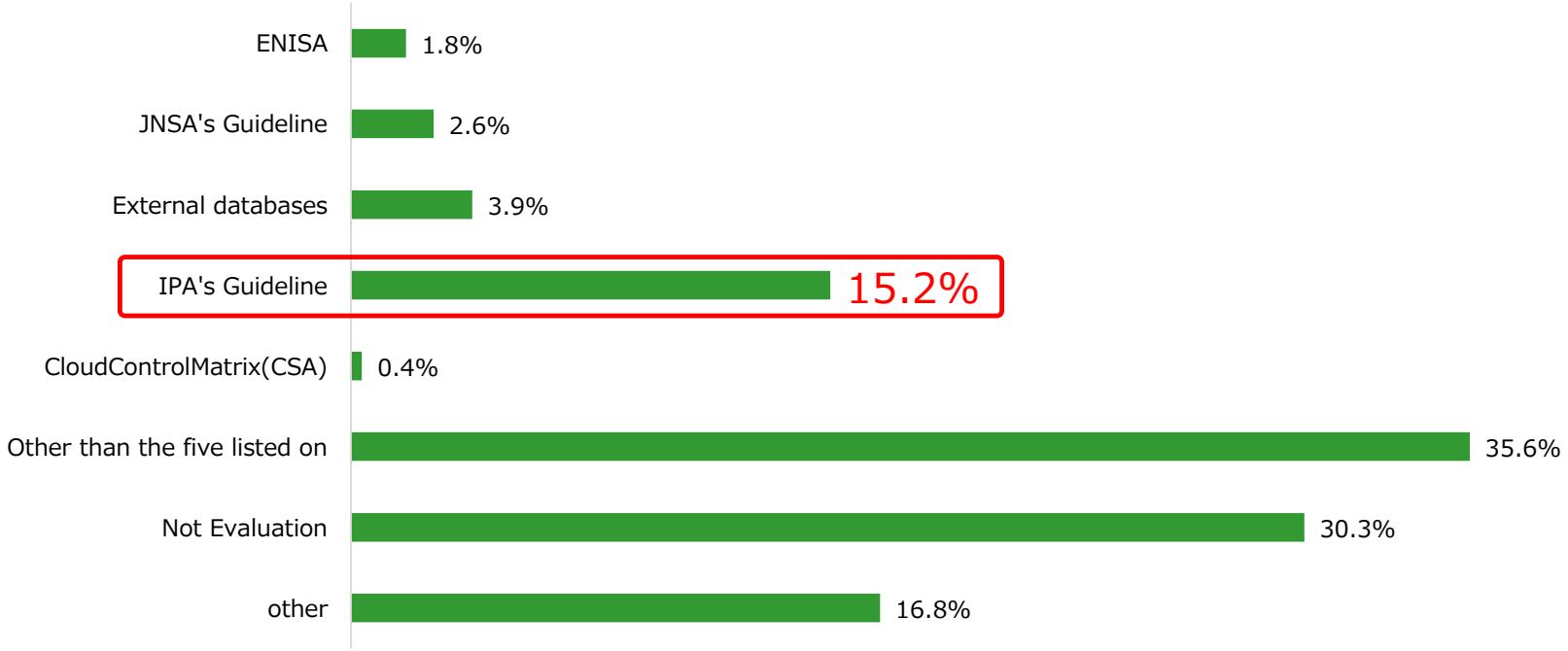
# Security Evaluation at Cloud Service Providers Selection (1/2)

Compared to the increasing trend from FY 2019 to FY 2020, the number of answers indicating that the company is evaluating the company was lower in FY 2020 to FY 2021.In FY2020, teleworking spread rapidly, internal assets were shifted to cloud services, and each company evaluated cloud service providers. **In FY2021, teleworking promotion settled down, but continued security evaluation is not considered to have taken root.**



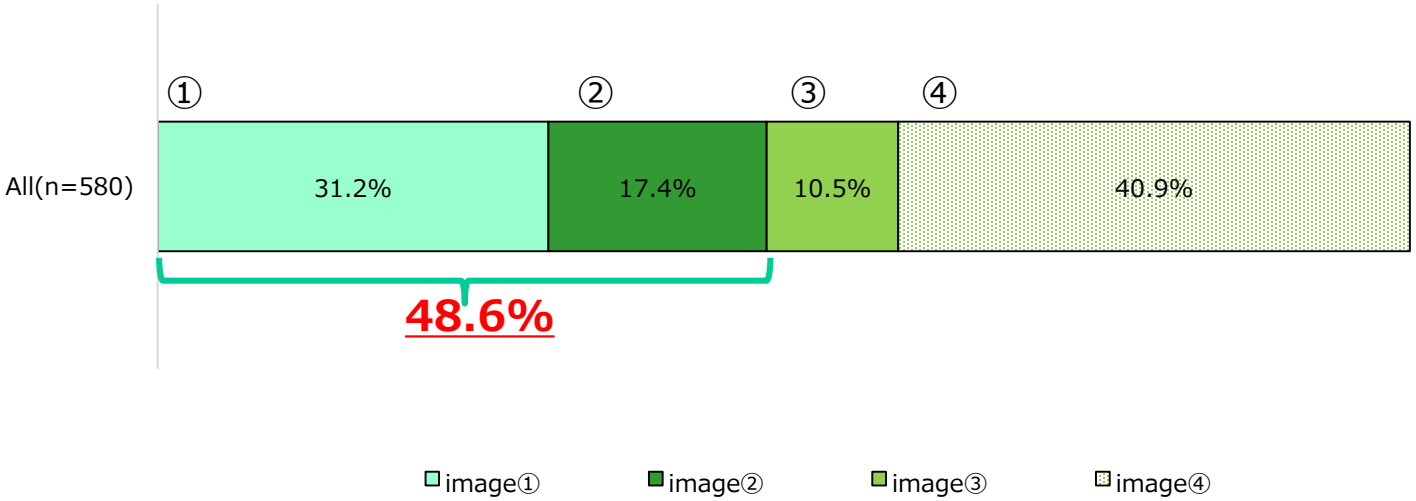
# Security Evaluation at Cloud Service Providers Selection (2/2)

Overall, the most common choice on the survey form was "I use the Guide to Secure Use of Cloud Services for SMEs (IPA)" (15.2%).
Other measures used for security evaluation included "third-party certification (ISO, SOC2, etc.)," "other company's use record," and a few answers that cited "ISMAP" as a measure used for security evaluation.

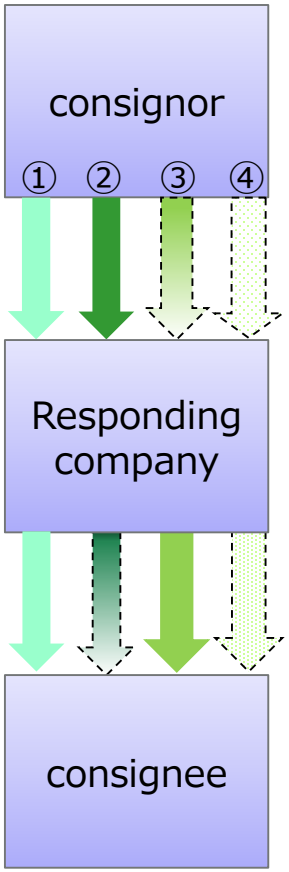


# Supply Chain Risk Management Status(1/3)

These days, corporate cyber risks have a significant impact not only on the company itself, but also on the supply chain in which it participates. In this survey, **48.6%(①+②)** of the total respondents answered that they are required to take cyber security measures by their supply chain.

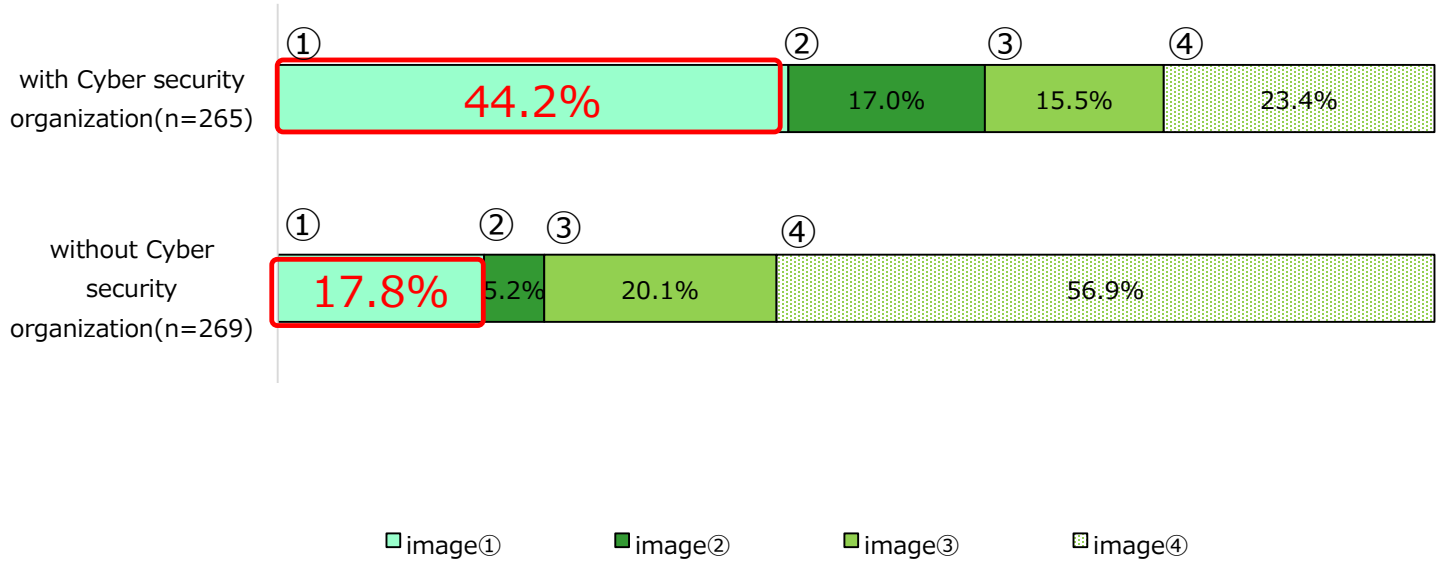



【image】

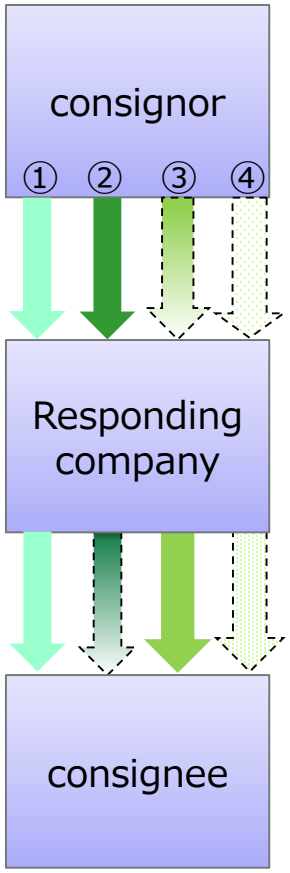


# Supply Chain Risk Management Status(2/3)

Among companies with an organizational structure, the percentage of companies that responded, "Our contractors require us to take cyber security measures, and we also require our contractors to take such measures," was 2.5 times higher than the percentage of companies that responded that they do not have an organizational structure.The percentage of companies that responded, "We request security checklists and other measures from our contractors. In some cases, the contractor company hastily established an organizational structure, while in other cases, the contractor company established an organizational structure in advance. In some cases, the company was able to meet the requirements smoothly by We believe that there are some cases.




【image】

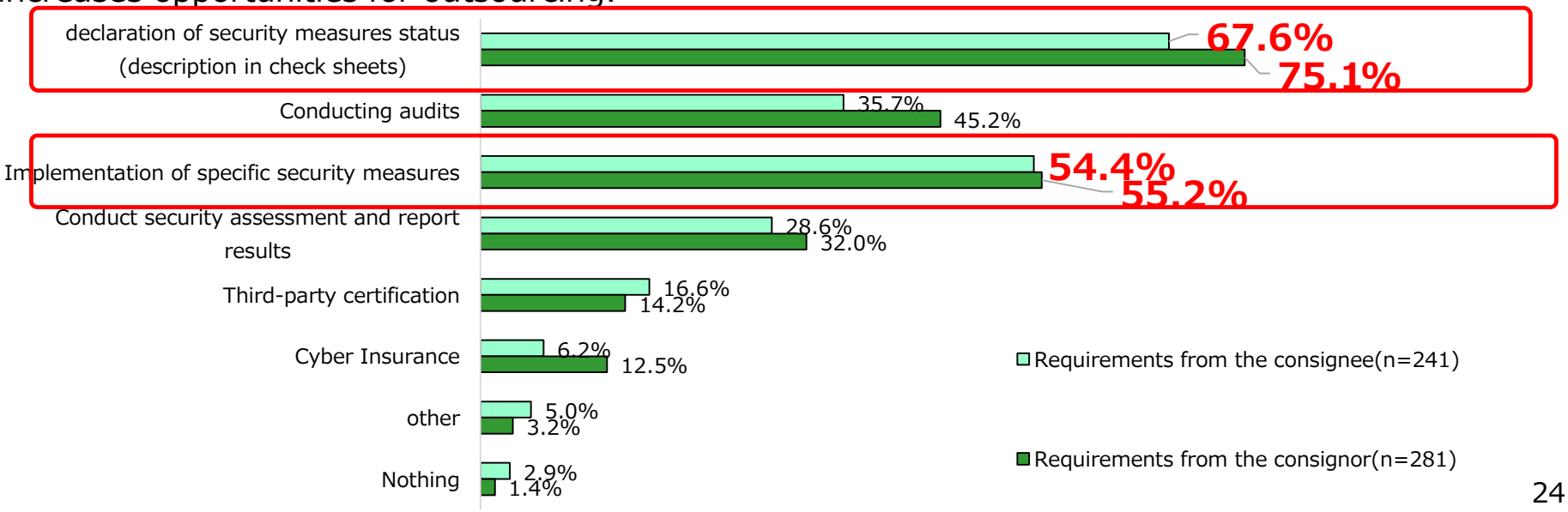


# Supply Chain Risk Management Status(3/3)

When asked about specific cyber security requirements among supply chain companies, the most common response for both requirements from the outsourcing source and requirements for outsourcing partners was "declaration of security measures status (description in check sheets)" (75.1% and 67.6%), followed by "specific security measures" (75.1% and 67.6%). Implementation" (55.2% and 54.4%).Based on these results, we propose the following roles for each company in the supply chain.

The consignor side should take the lead in strengthening the entire supply chain system by requesting cyber security measures from the outsourcing partner companies, thereby realizing a sustainable and stable supply chain.

The consignee side should prepare a cyber security organization system in advance to meet the ever-increasing demand for cyber security measures among supply chain companies and establish a system for outsourcing business. This not only strengthens the company's own cyber countermeasures, but also has the direct business benefit of increasing corporate value, which increases opportunities for outsourcing.

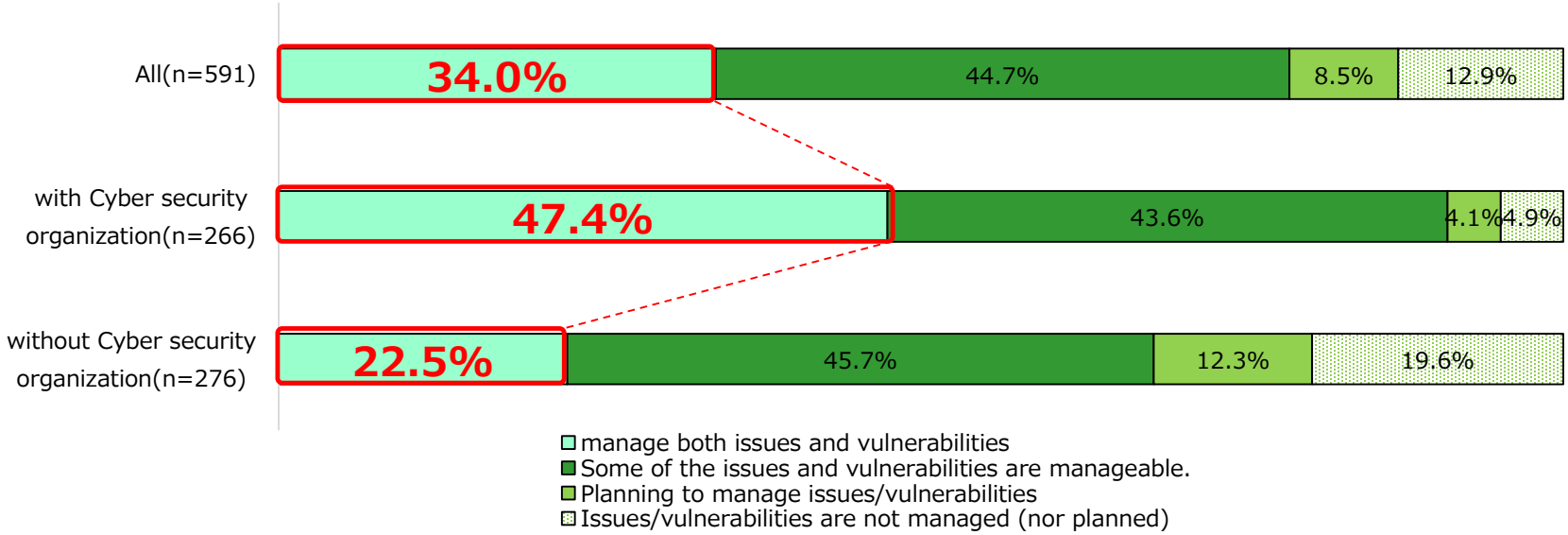


# Identify

# Issues with information assets held

(e.g., confidential information is placed where anyone can refer to it, passwords are not encrypted, etc.)

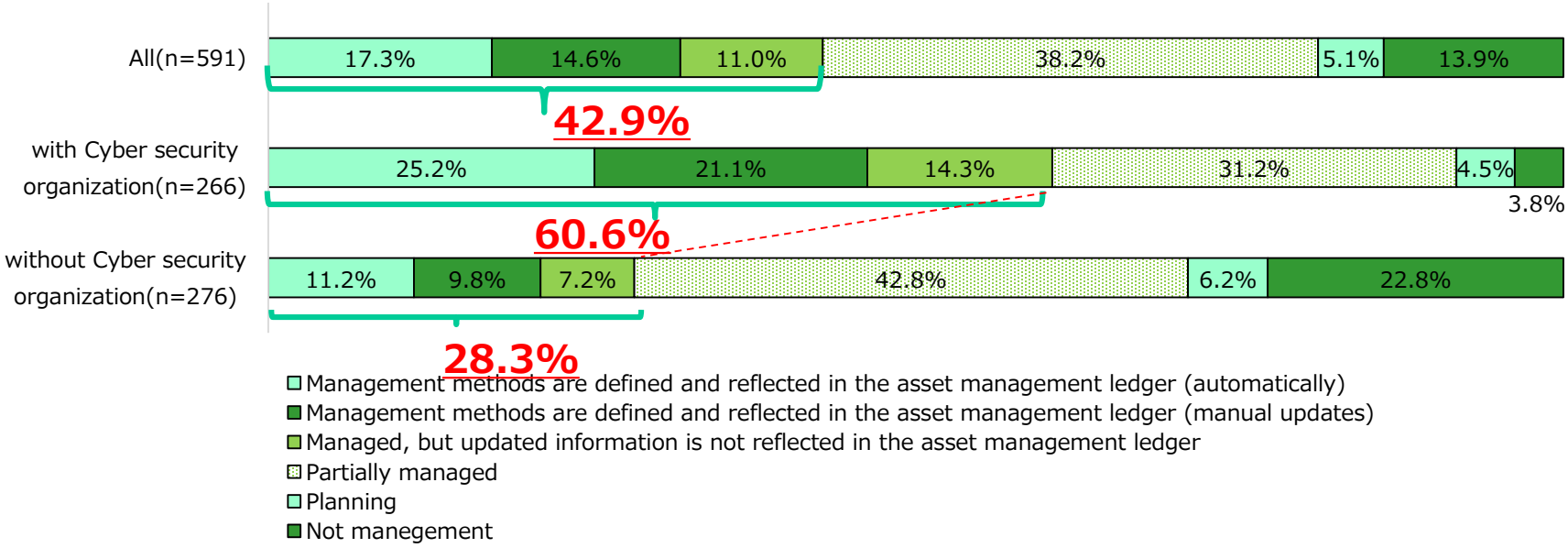
Overall, **only 34.0% of companies answered that they manage both issues and vulnerabilities.**When this question was asked by cybersecurity organizational structure, **47.4% of companies with cybersecurity organizational structure answered that they "manage issues and vulnerabilities," while 22.5% of companies without cybersecurity organizational structure answered that they "manage issues and vulnerabilities.** A large difference was observed depending on whether or not a company has a cybersecurity organizational structure.



# Vulnerability management

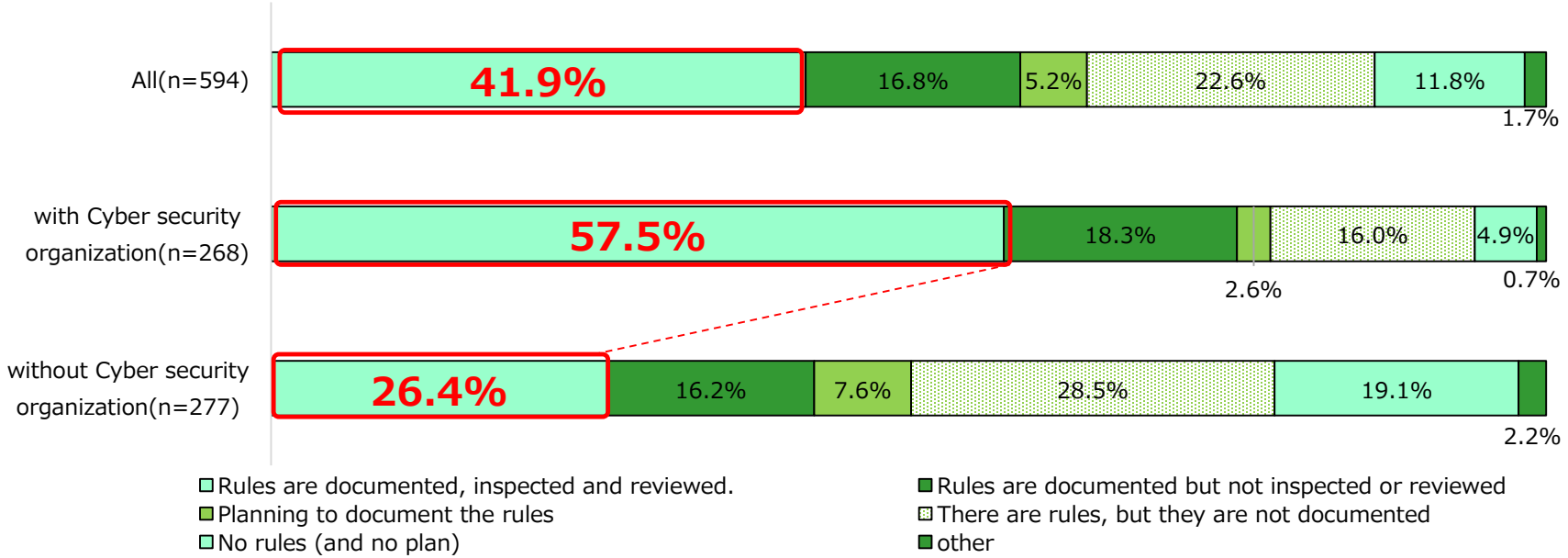
(e.g., Vulnerabilities in Windows, Adobe Flash, etc.)

The total number of responses that manage vulnerabilities (“Management methods are defined and reflected in the asset management ledger (automatically or manual updates)" and "Managed, but updated information is not reflected in the asset management ledger") was **42.9%.**A particularly large difference was observed between those with and without a cyber security organizational structure, **at 60.6% and 28.2% respectively**.Cyber-attacks that exploit vulnerabilities have recently been attracting attention as a major threat, and companies are required to manage vulnerabilities in their cyber security organizational structure.



## Develop rules for user IDs, passwords, and authorization to view and update information

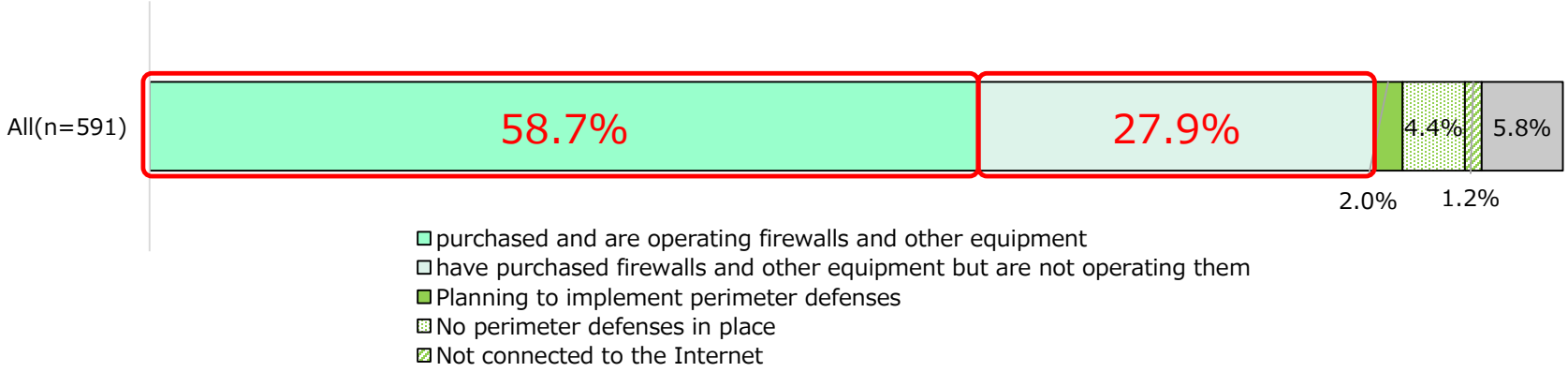
**About half (41.9%) of all companies answered that they have documented rules for IDs, passwords, and updating information references**, and that these rules are checked and reviewed. The percentage of companies with a cyber security system was **57.5%**, while the percentage of companies without a cyber security organizational structure was **26.4%**, which is a large discrepancy. " Other" included "No rules, but inspections are conducted," "Dependent on/compliant with parent company", and "Only computers that handle personal information" are inspected.



# Detection, protection, response, and recovery status

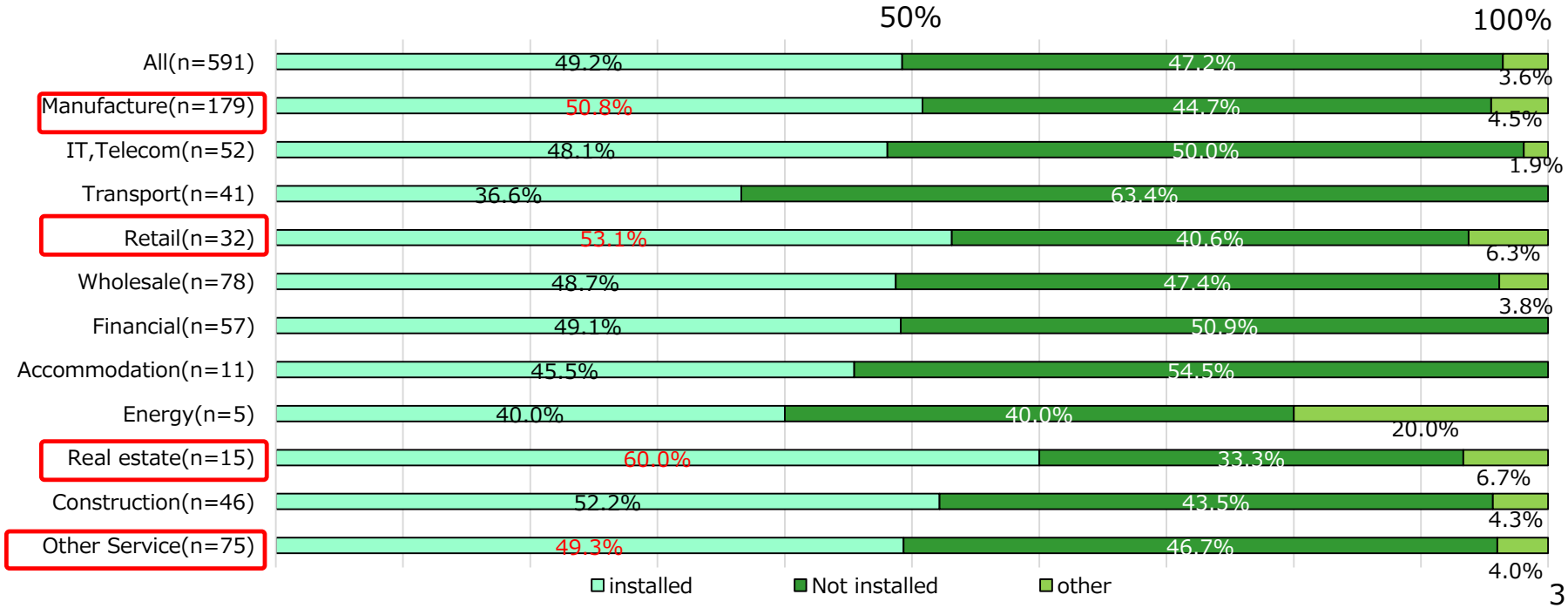
## Boundary protection between the Internet and the company's own network (e.g., firewalls)

We checked the status of implementation of boundary protection between the Internet and the company's own network. Overall, **more than half of the companies (58.7%) have purchased and are operating firewalls and other equipment**.On the other hand, 27.9% of companies "have purchased firewalls and other equipment but are not operating them" indicating that they are unable to respond immediately to cyber attacks or to fully demonstrate the effectiveness of their security products and services, and that issues remain regarding the effectiveness and efficiency of their **countermeasures.For companies that do not have the resources to operate their own systems, it is recommended that they introduce a "managed security service (MSS)" that provides one-stop services, including monitoring and incident response.**



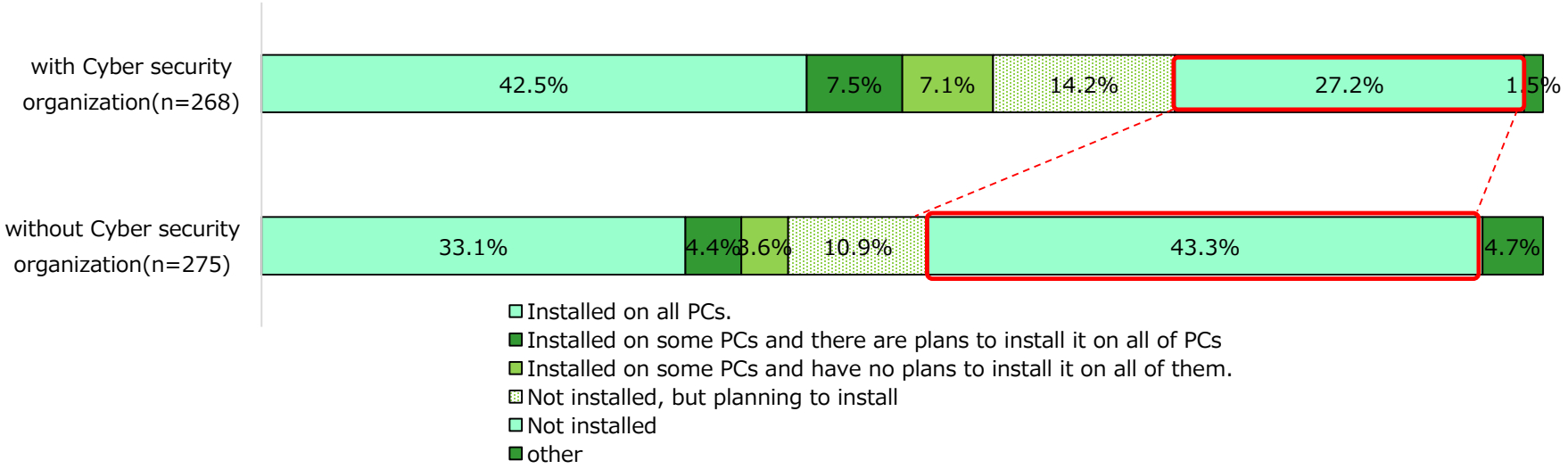
## Deployment of EDR (1/2)

Regarding the status of EDR (Endpoint Detection and Response) implementation, **49.2% of all companies answered that they have implemented EDR (total number of "implemented on all PCs" and "on some PCs")**. When broken down by industry, **the real estate (60.0%), retail (53.1%), manufacturing (50.8%), and other services (49.3%) industries exceeded the overall average.**



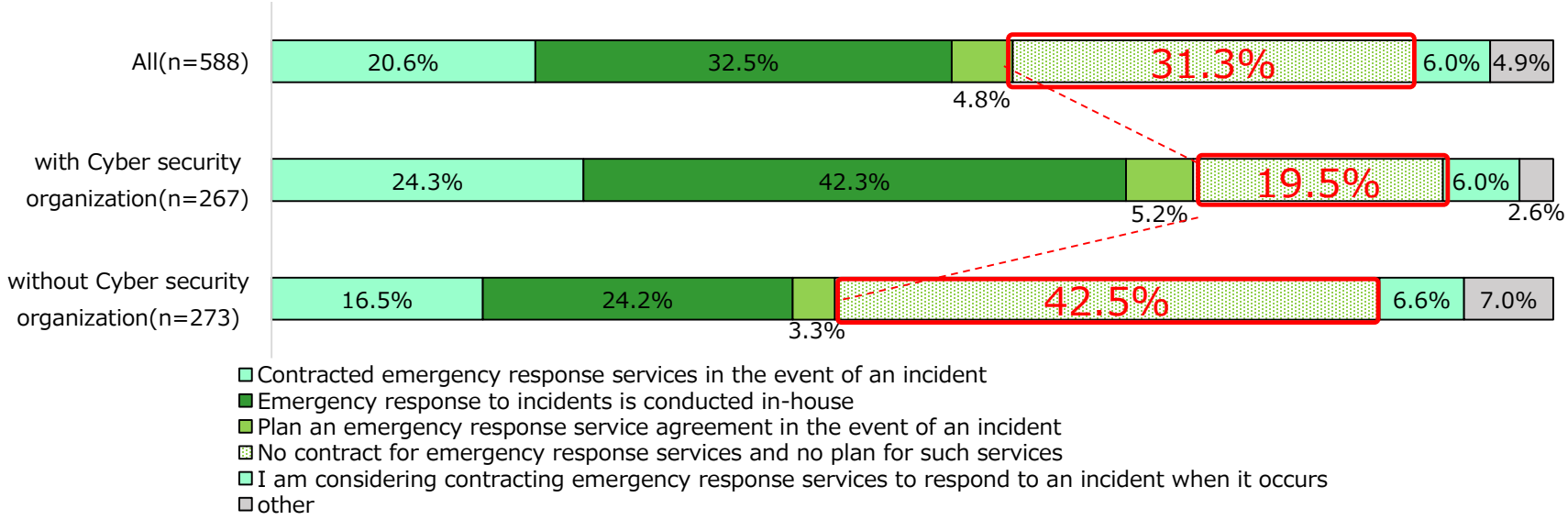
## Deployment of EDR (2/2)

When this question was asked by cyber security organizational structure, the percentage of companies without an organizational structure that answered **" Not installed " was approximately 1.6 times higher** than that of companies with organizational structure.For companies without an cyber security organizational structure, **outsourcing EDR security operations through Managed Security Services (MSS) has the advantage of simultaneously strengthening the security structure and countermeasures.**



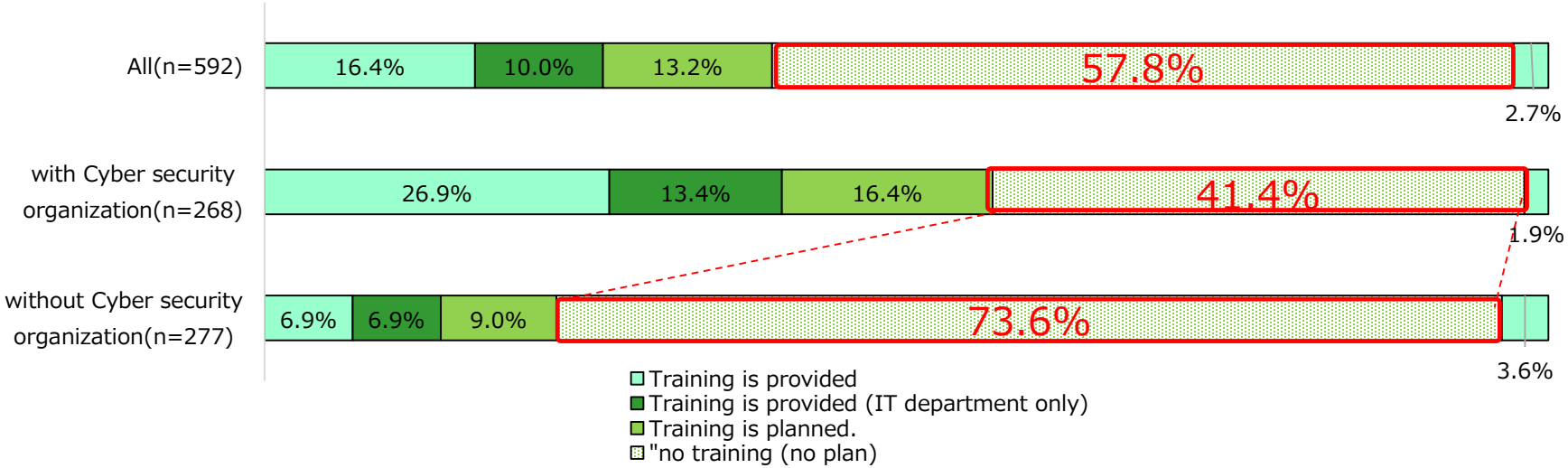
## Contracts for emergency support services, etc. in the event of a security incident (accident)

There was a large difference in the response rate for **" No contract for emergency response services and no plan for such services "** by Cyber Security organizational structure status.In cases where cyber security systems are not yet in place or where budget and personnel allocation are difficult, **there is significant potential for proactive use of services such as referrals to specialized providers that are included in cyber insurance policies in the event of an accident.**



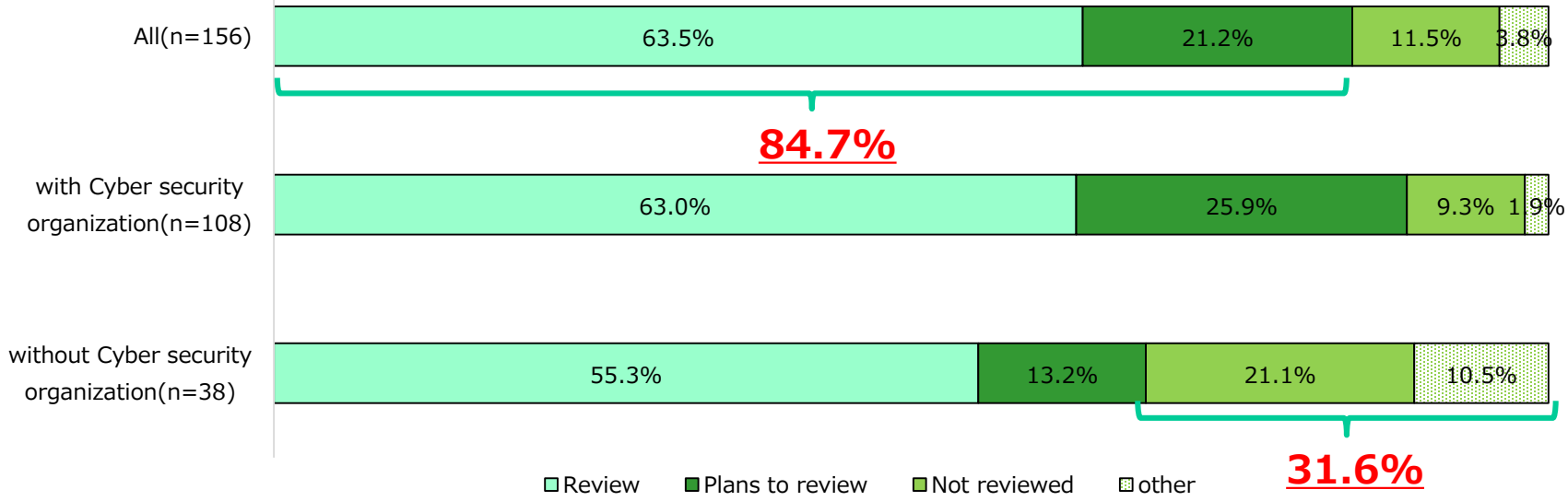
# Status of security incident training

Regarding whether they conduct training in the event of a security incident, the majority **(57.8%)** of all companies answered that they "no training (no plan)".When this question was examined by the presence or absence of a cyber security organizational structure, there was a divergence in the percentage of respondents who answered "no training (no plan)" depending on the presence or absence of an organizational structure. Companies with an organizational structure are able to make appropriate judgments and responses as an organization, and to respond to security incidents while also making use of past experience. For companies that do not have an organizational structure, **it is desirable for them to develop an organizational structure, including incident training, and to strengthen the structure, including outsourcing of incident response.**



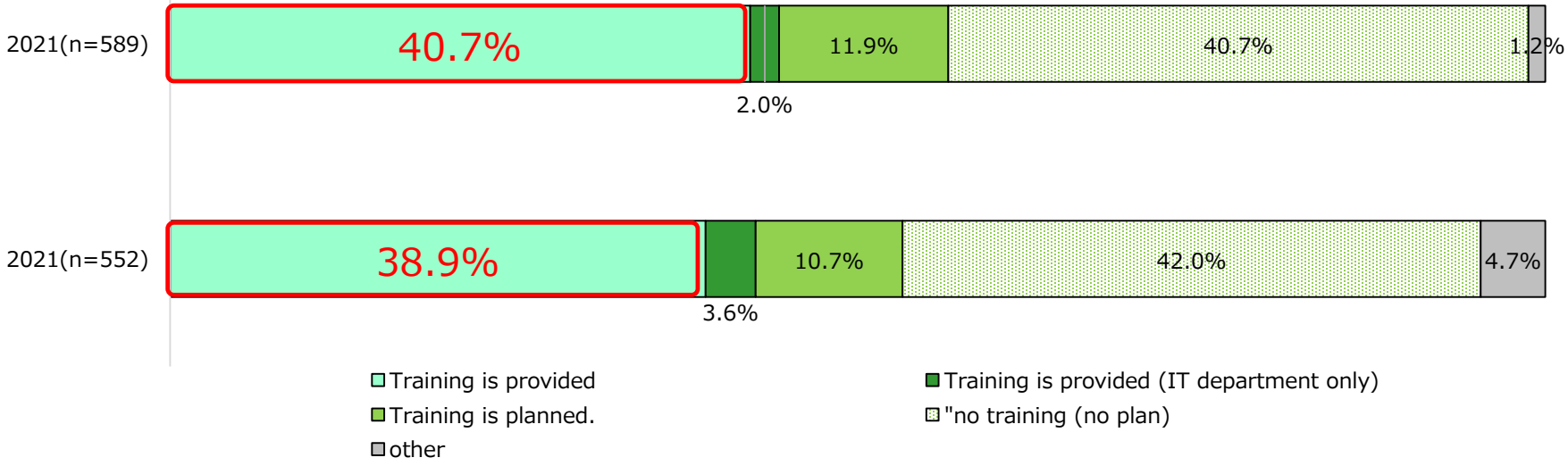
# Whether or not the results of security incident training are reviewed.

**63.5%** of all companies are reviewing the results of their training and the content of their training, and including those that "Plans to review" **(21.2%)**, the number of companies that have reviewed or plan to review the content of their training exceeds 80%.On the other hand, about **30% of companies without a cyber security organization have not reviewed their training.**



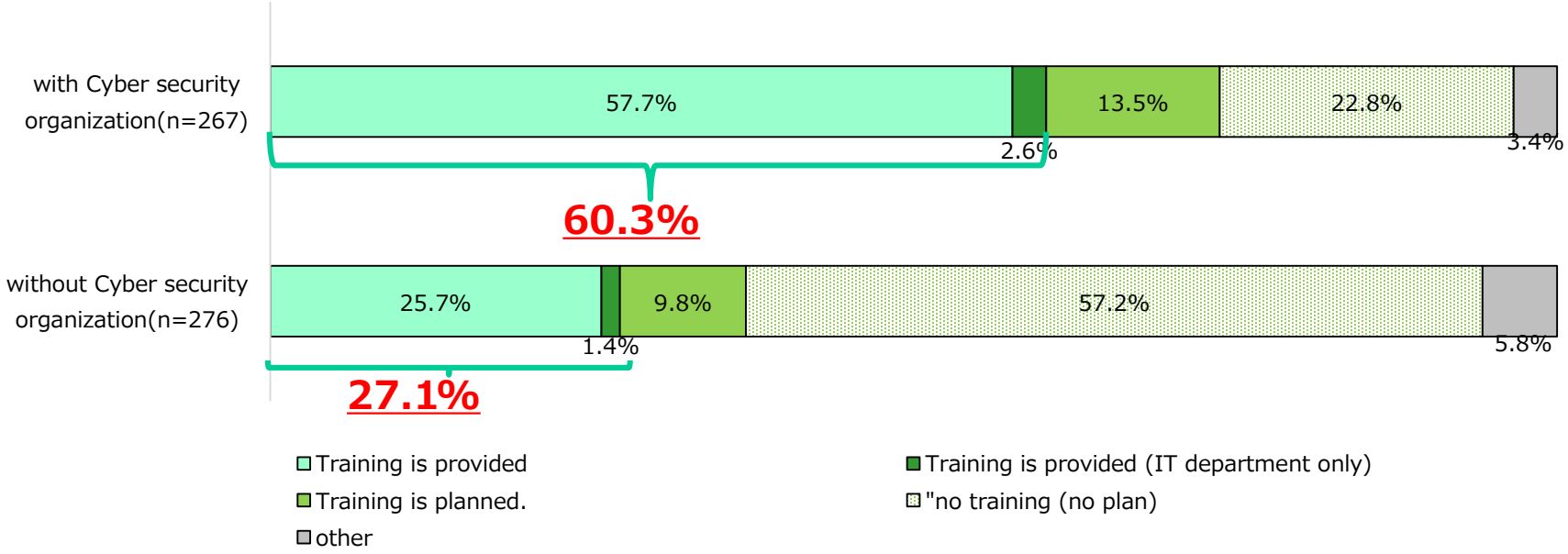
# Implementation status of training for incoming Fishing Emails(1/2)

Regarding whether they conduct training on incoming Fishing Emails, **40.7%** of the total respondents answered that they "Training is provided“. This is a slight increase from the results of the FY2020 survey and suggests that company-wide training is gradually spreading.Also, compared to the aforementioned security incident training, which is a broad topic, a higher percentage of respondents conduct training, suggesting that Fishing emails have become a more familiar threat to companies.



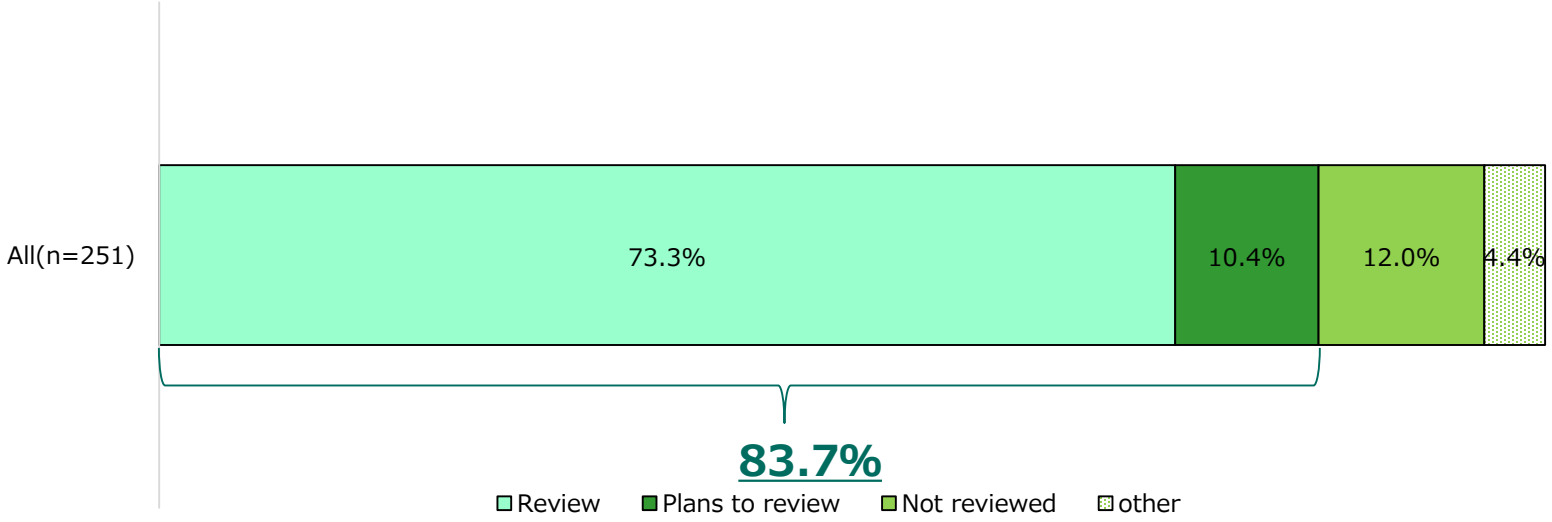
# Implementation status of training for incoming Fishing Emails(1/2)

Many companies with an Cyber Security organizational structure **(60.3%)** answered that they "conduct training (the total number of companies with non-IT department participation and IT department participation only). On the other hand, less than **27.1%** of the companies without an Cyber Security organizational structure answered "Yes" to this question.**Establishing an organizational structure as well as security incident training is the first step in strengthening the subsequent security structure.**



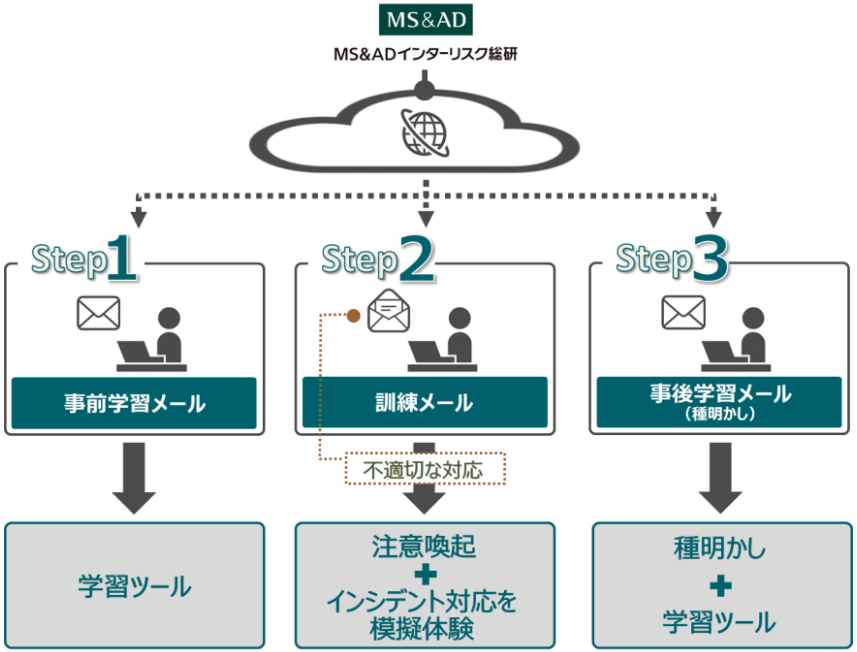
## Whether or not the results of training for Fishing Emails have been reviewed (1/2)

Including those companies that are planning to review Fishing Emails training **(10.4%)**, more than **80%** of the companies have reviewed or are planning to review their training **content.In Fishing Emails attacks, it is difficult to reduce the open rate to zero, so it is important to educate and train employees so that they can quickly and appropriately report and take other actions when they do open an email.**



## Whether or not the results of training for Fishing Emails have been reviewed (2/2)

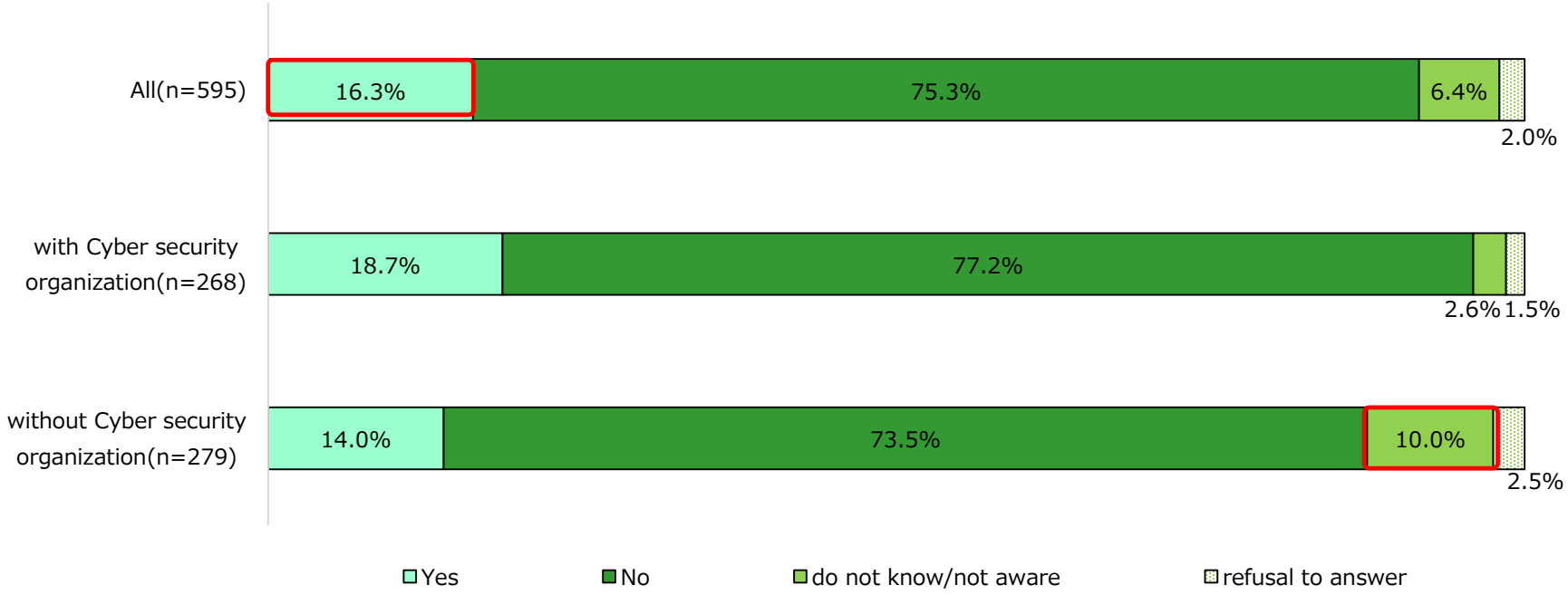
Fishing Emails training service we provide comes in two types: a full package plan that includes "pre-learning," "training e-mails," and "post-learning," and a plan that includes only training e-mails. The fact that the full package plan accounts for more than 70% of the service offerings suggests that **there is a need for training that includes actions to be taken when targeted emails are opened.**



# Cyber Security Incidents

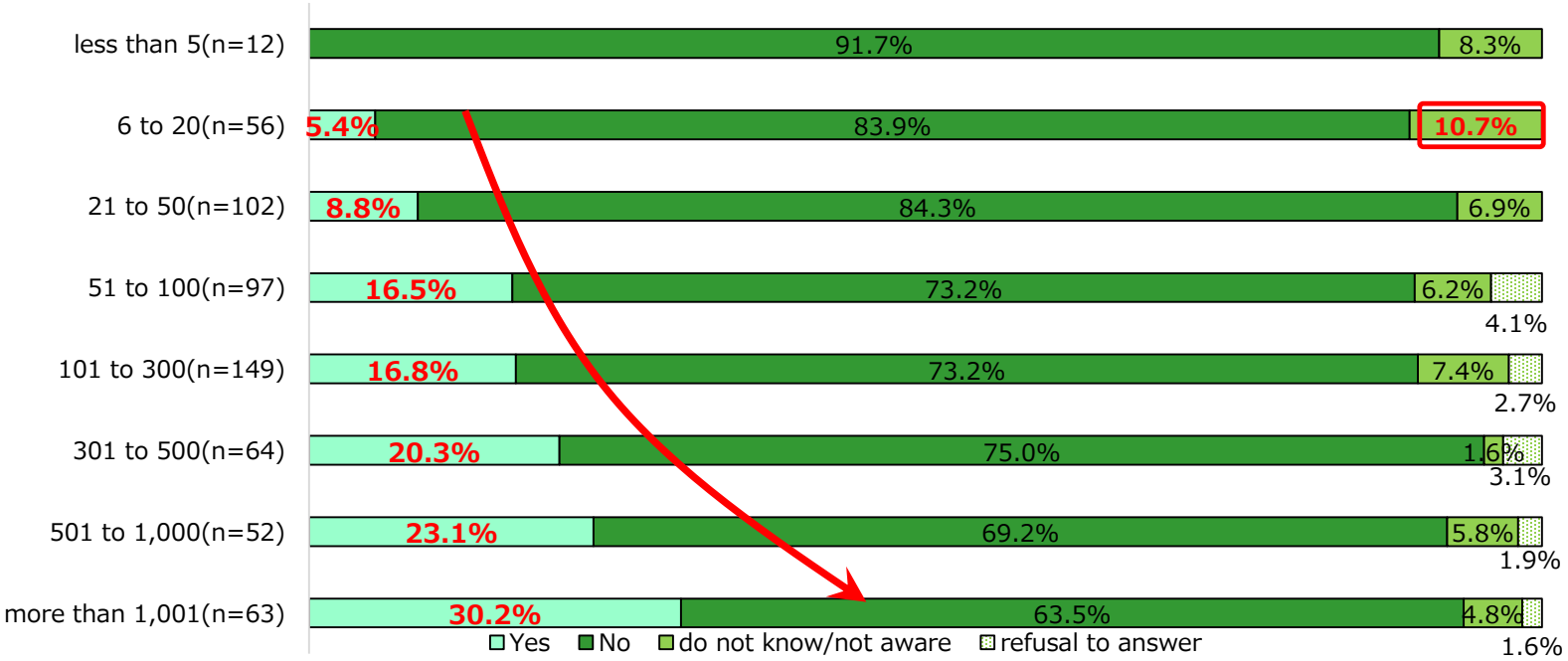
# Past cyber security incidents (1/2)

When asked if there had been any cyber security incidents in the past, **16.3%** of the companies answered “Yes". By cyber security system, a higher percentage **(10.0%)** of companies without an organizational structure answered that they "do not know/not aware," **suggesting that they may not have detected the incident even if it had occurred in the first place.**



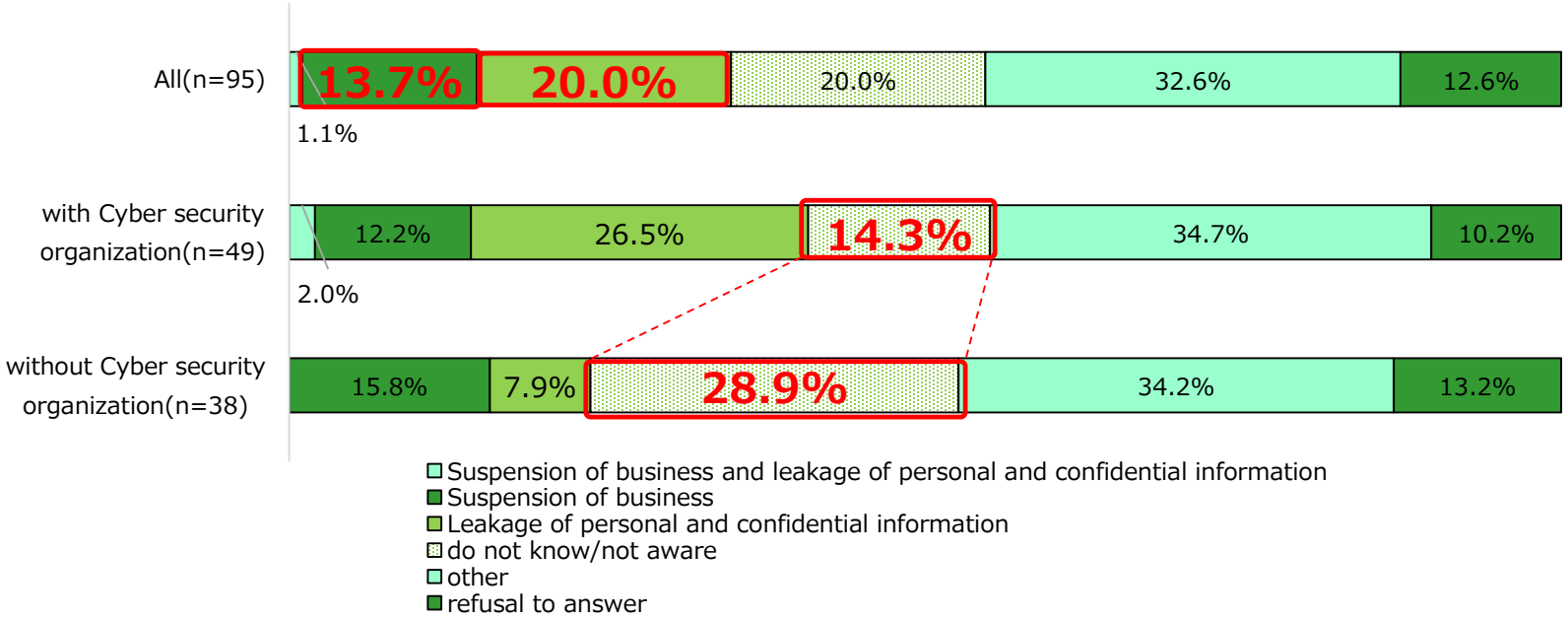
# Past cyber security incidents (2/2)

The percentage of companies that answered that **there were incidents was higher for companies with a larger number of employees**.It can be inferred that large companies are more likely to experience cyber attacks as the ultimate goal of targeted attacks and supply chain attacks, in addition to indiscriminate attacks.
In addition, **10.7%** of companies with 6 to 20 employees answered that they "do not know" or "do not understand," **suggesting that they may not have detected the incident even if it had occurred in the first place.**



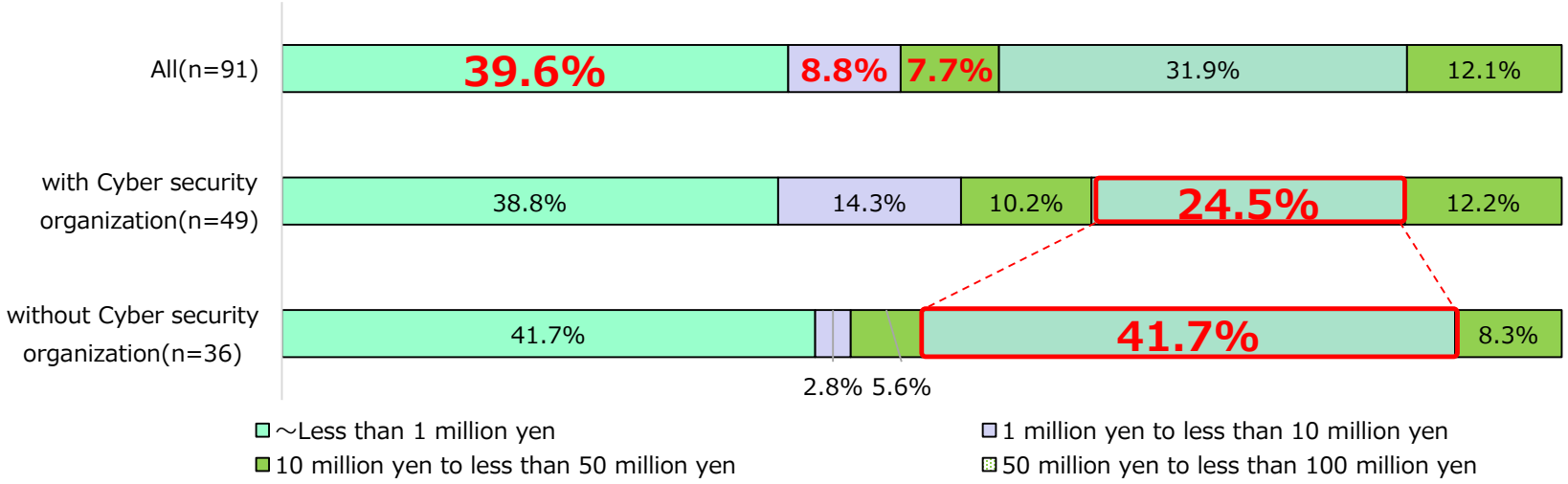
## Details of the most damaging cybersecurity incidents

When asked about the most damaging cyber security incidents in the past, the most common answer was leakage of personal and confidential information **(20.0%)**, followed by business shutdown **(13.7%)**.For this question, the percentage of respondents who answered "Do not know/not aware" varied nearly twice as much depending on whether or not a cyber security system was in place. **We believe that having a cyber security system in place at normal times will be helpful in understanding the situation in the event of an emergency.**



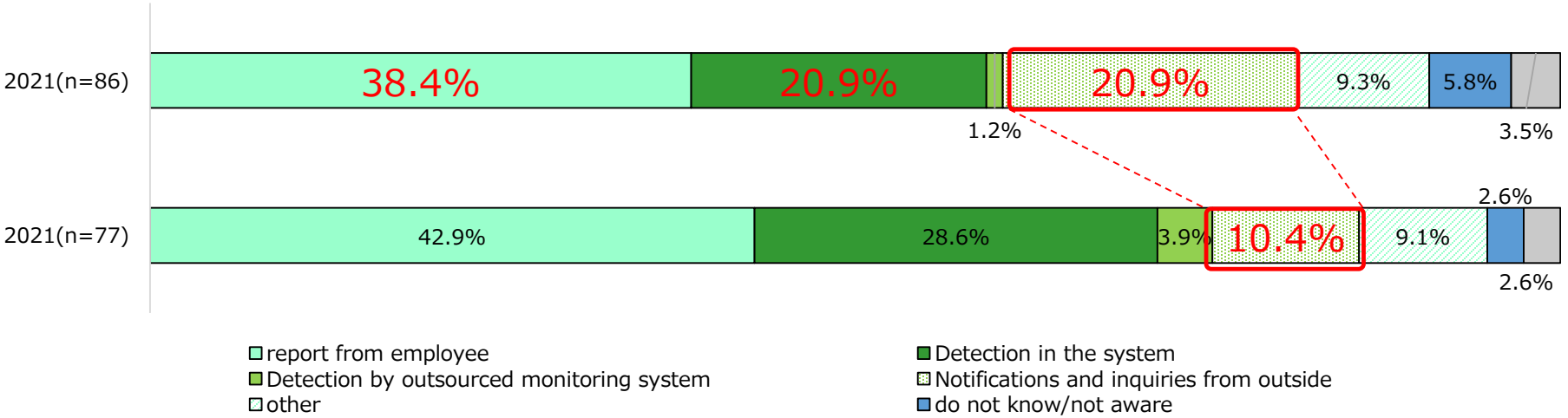
# Amount of losses from the most damaging cybersecurity incidents

When asked to confirm the amount of damage caused by the most damaging cyber security incidents in the past, **39.6% of the respondents reported losses of less than 1 million yen, followed by 1 million to 10 million yen (8.8%) and 10 million to 50 million yen (7.7%)**.Again, the percentage of respondents who answered "do not know/not sure" varied about twice as much depending on whether or not they have a cyber security system.



# Reason for recognizing the incident

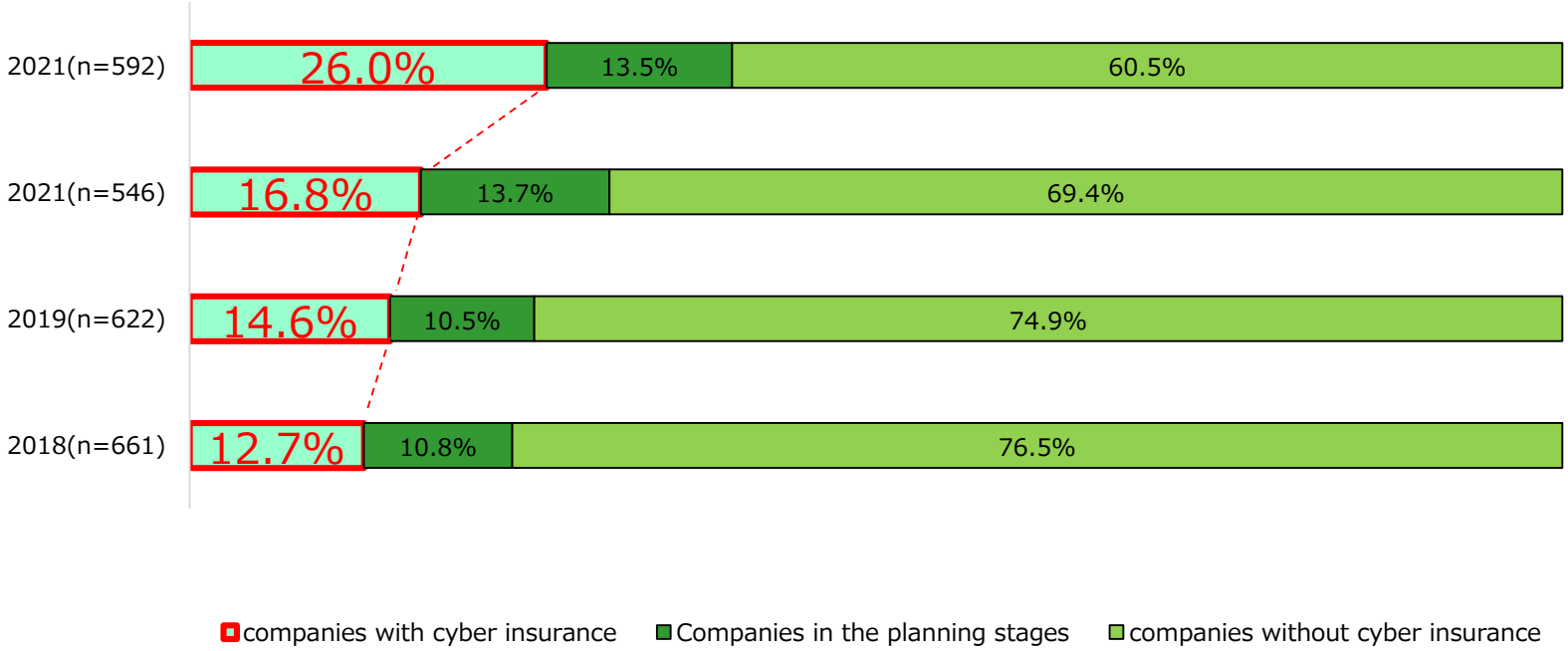
“How the enterprise recognized the accident?”.
The results were as follows:
1st “report from employee”
2nd” Detection in the system”, “Notifications and inquiries from outside”
Compared to FY2020, the percentage of responses for "notification or inquiry from outside the company," such as from the police or security vendors, increased (from 10.4% to 20.9%).In order to minimize damage, it is desirable to "detect cyber-attacks in-house" and "respond promptly and appropriately.



# Cyber Insurance

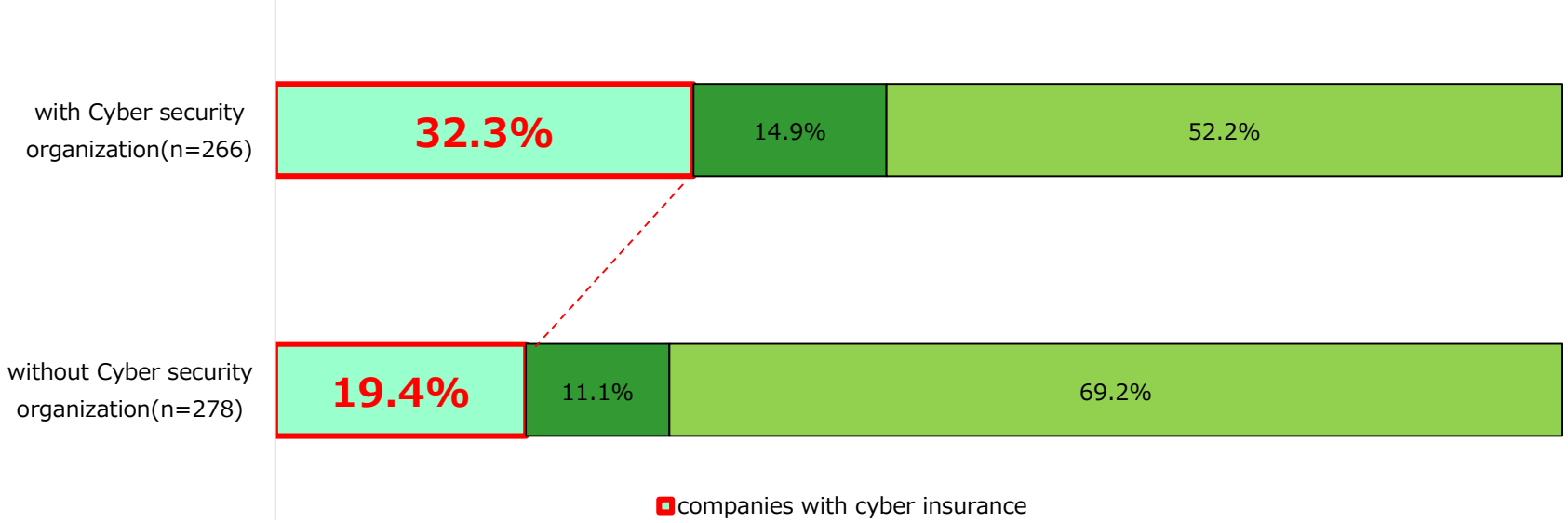
# Status of cyber insurance(1/2)

Overall, the percentage of companies with cyber insurance is low at **26.0%**, but compared to the results of the previous years' surveys, **the percentage of companies with cyber insurance has been increasing every year, especially in FY2021, more than the trend has been.**



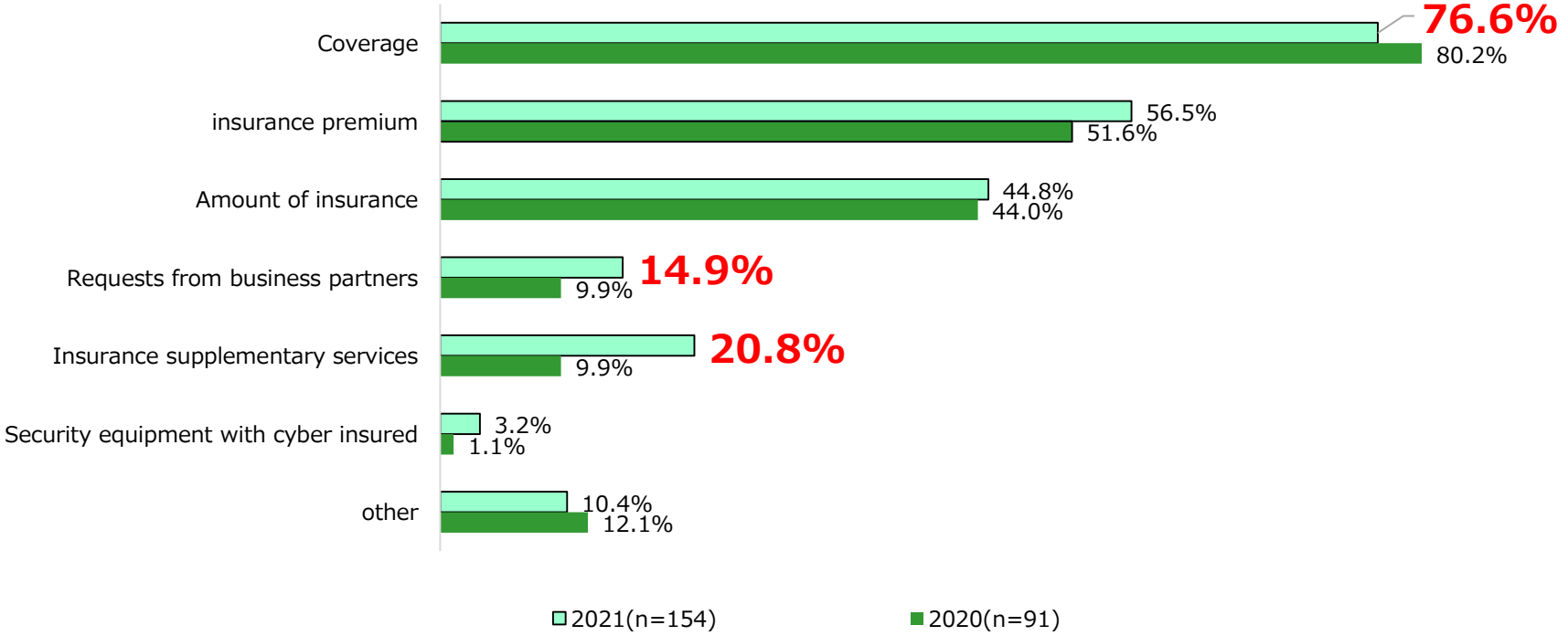
# Status of cyber insurance (2/2)

A difference in Purchase ratio  was observed when checking by the presence of a Cyber Security organizational structure. The company rate who has cyber insurance policy with an Cyber Security Tema was **32.3%**, while the rate for who has insurance policy without a Cyber Security organizational structure was **19.4%**, **a difference of 1.5 times the rate for those without a structure.**



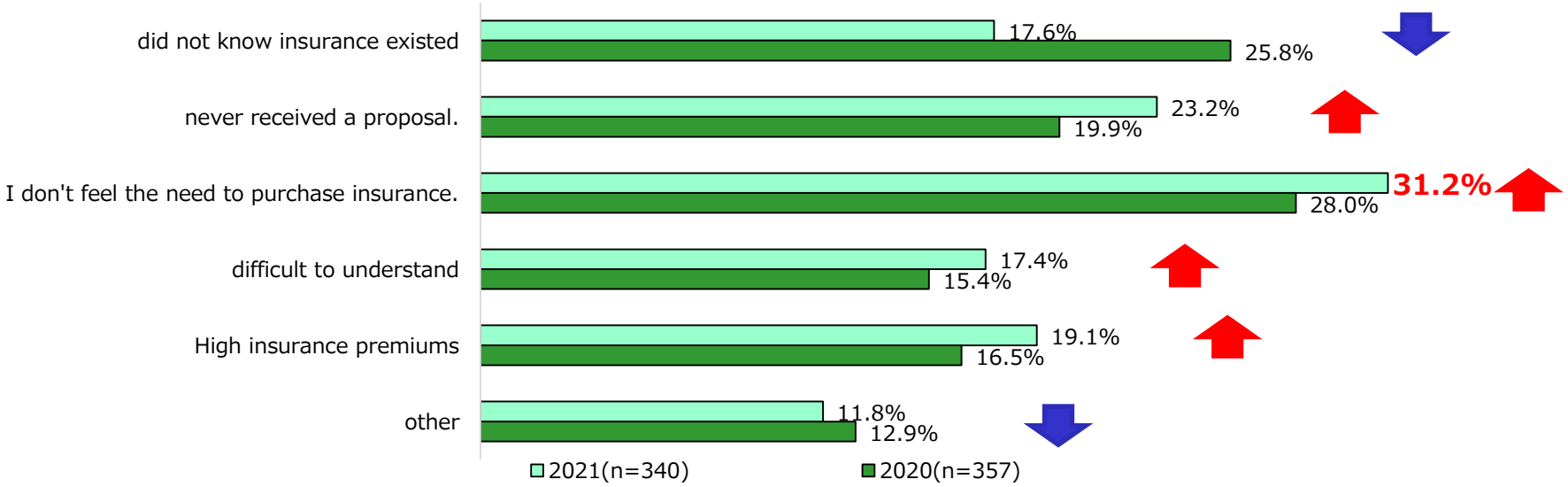
# The reason who have policy * Multiple selection

The most common reason given for purchasing cyber insurance was "coverage suited to my company" (76.6%).Compared to last year's answer rate, there was a particular increase in the percentage of respondents who answered "request from business partners" **(from 9.9% to 14.9%)** and "supplementary insurance services" **(from 9.9% to 20.8%)** as reasons for their decision.



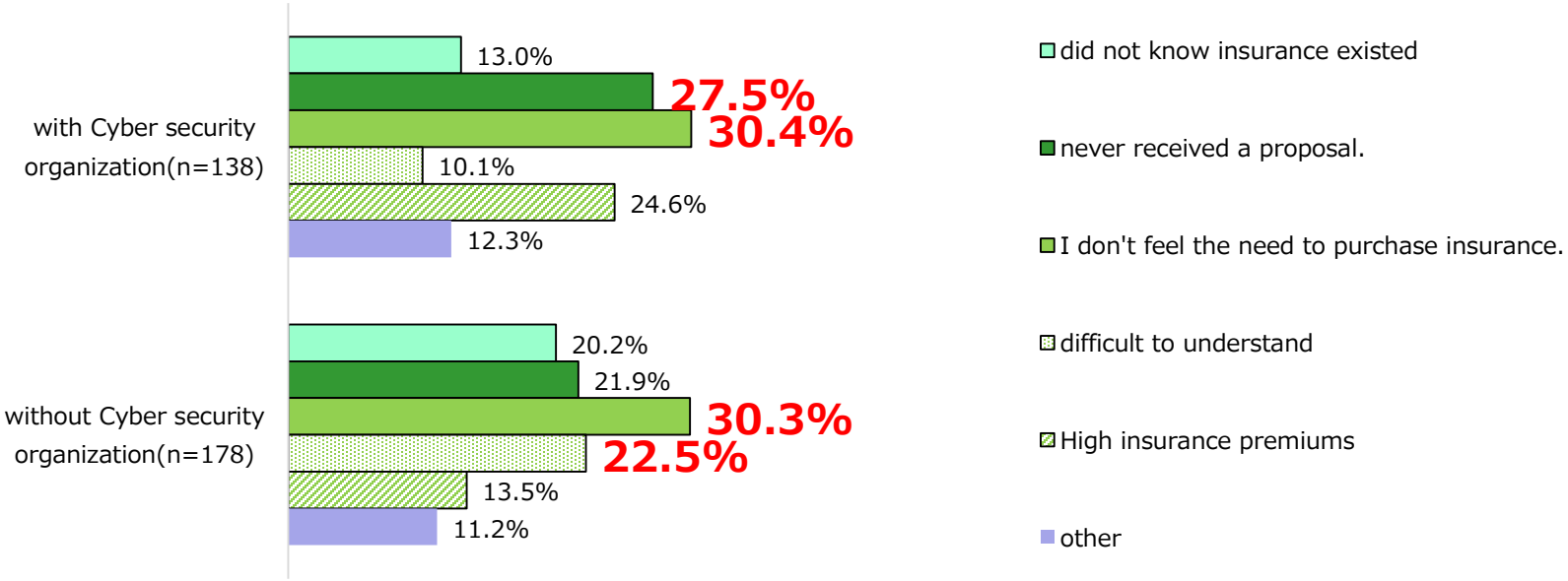
# The reason who don’t have policy * Multiple selection(1/2)

Compared to last year's survey, the most common answer for not having cyber insurance was "do not feel the need to purchase insurance **(31.2%)**.Compared to last year's response rate, **the percentages of "did not know insurance existed" and "other" decreased, while the percentages of all other responses increased**.While the awareness rate of cyber insurance is increasing, **the number of companies that do not feel the need to purchase cyber insurance is also increasing.**



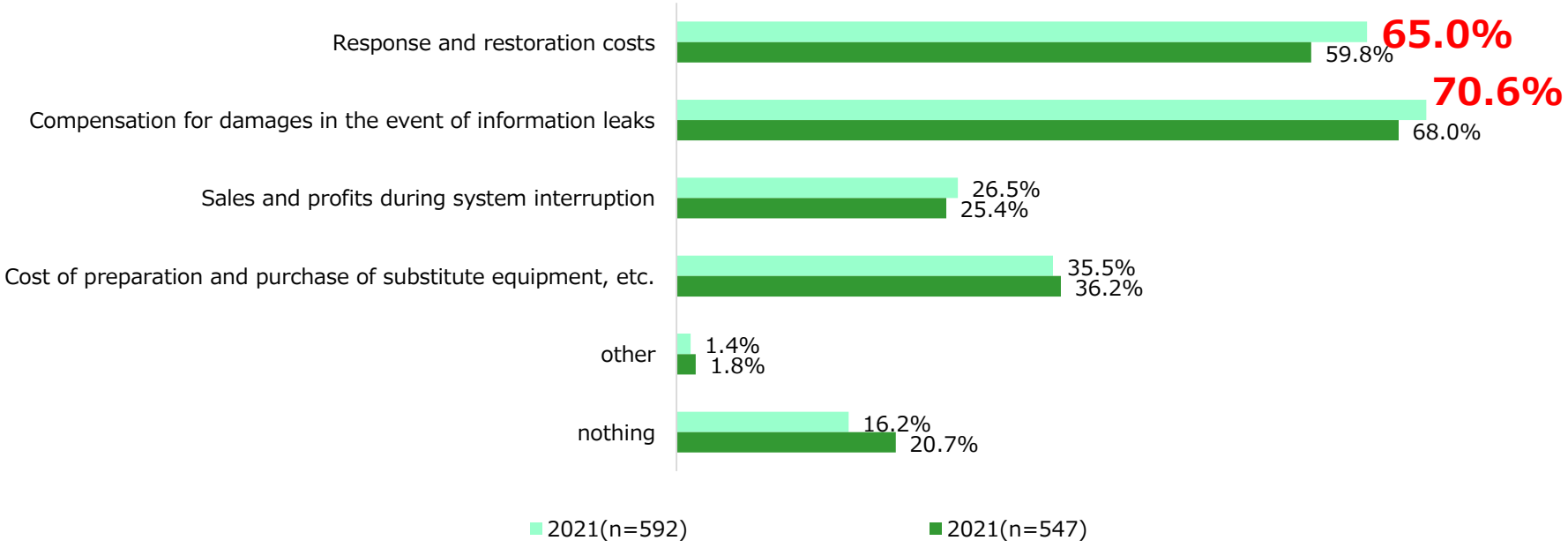
# The reason who don't have policy * Multiple selection(2/2)

When asked by Cyber Security organizational structure, the most common answer among companies with organizational structure was **"I don't feel the need to purchase insurance" (27.5%)**, followed by **"I knew there was insurance, but I have never received a proposal" (27.5%)**.On the other hand, in the absence of organizational structure, the most common response was the same, but the second most common response was **"I don't know what insurance is or it is difficult" (22.5%).**



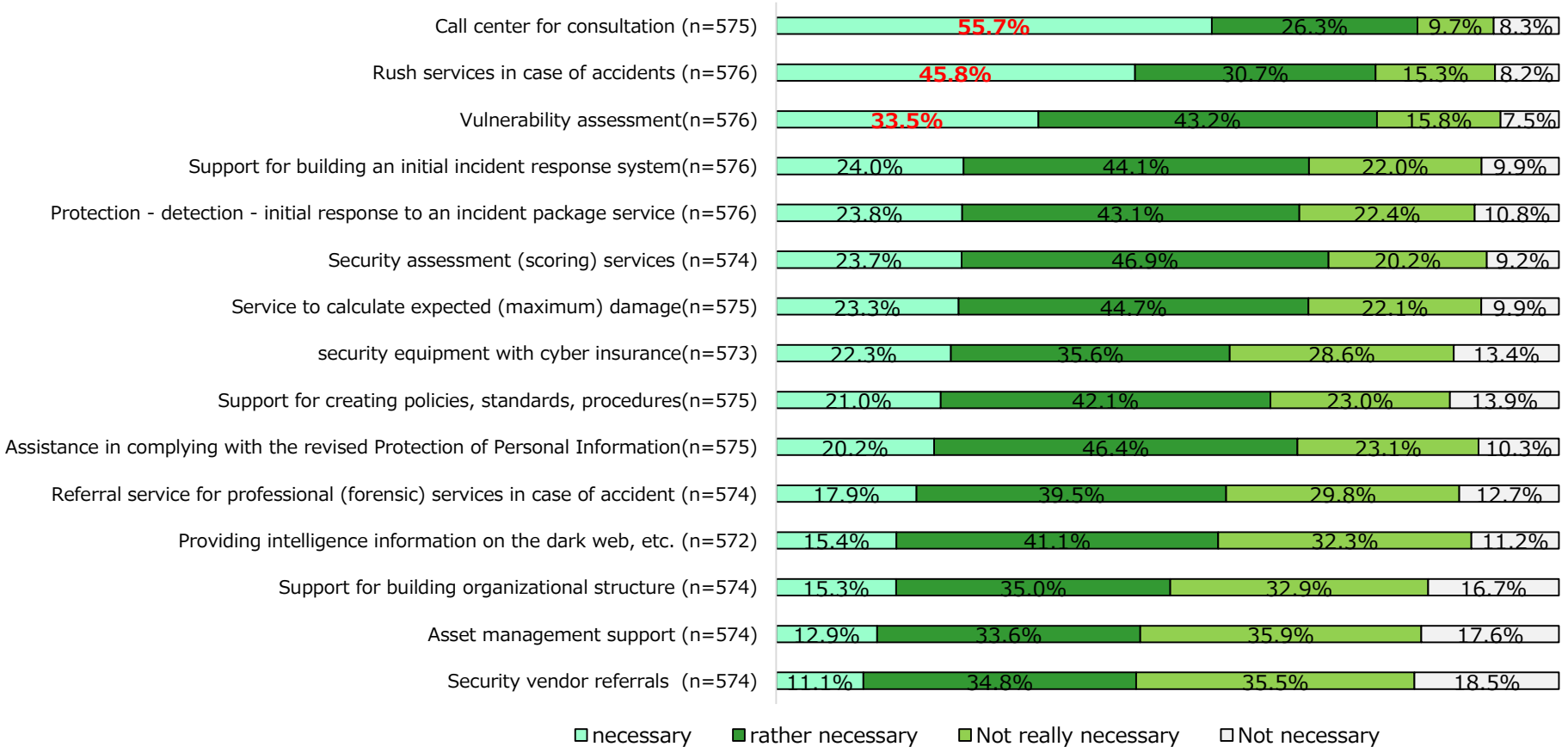
# Required coverage * Multiple selection

The most common loss expected to be covered by insurance was **"compensation for damages at the time of information leakage" (70.6%)**, 2nd is **"response/restoration costs" (65.0%).**Compared to the response rate in the previous year, there was no significant change in the response trend.



# Expectations for additional insurance services(1/3)

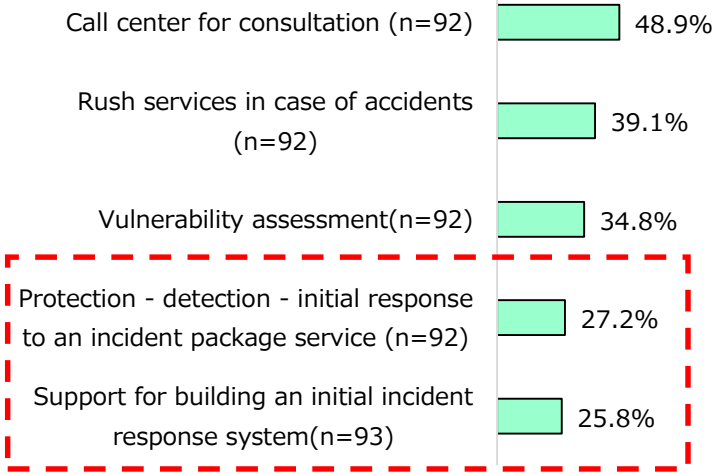
Expected services, in particular, were **"call center for consultation (55.7%)," "rush service in case of accidents (45.8%),"** and **"vulnerability assessment (33.5%),"** in that order.



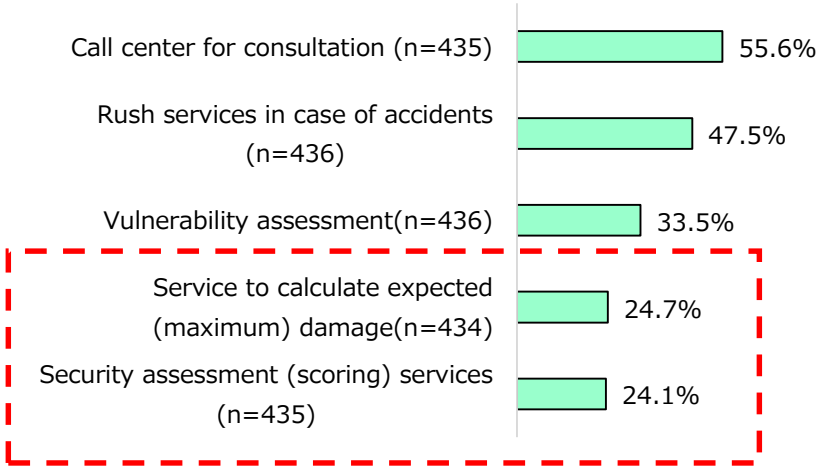
# Expectations for additional insurance services (2/3)

When compared to the answers for "necessary" in terms of ancillary services by cyber accident status, the first three responses were the same, but the fourth and fifth responses were services related to accident response for companies that have experienced cyber accidents, and services related to cyber security scoring and diagnosis for companies that have not experienced cyber accidents.The percentage of respondents who answered that a call center for consultation and a rush service at the time of an accident are "necessary" was slightly lower among those with cyber accident experience. **The results show that the need for supplementary services differs depending on the company's experience with accidents.**

**Expectations for additional insurance services**
( Experienced cyber incidents )




**Expectations for additional insurance services**
(Not experienced cyber incidents )



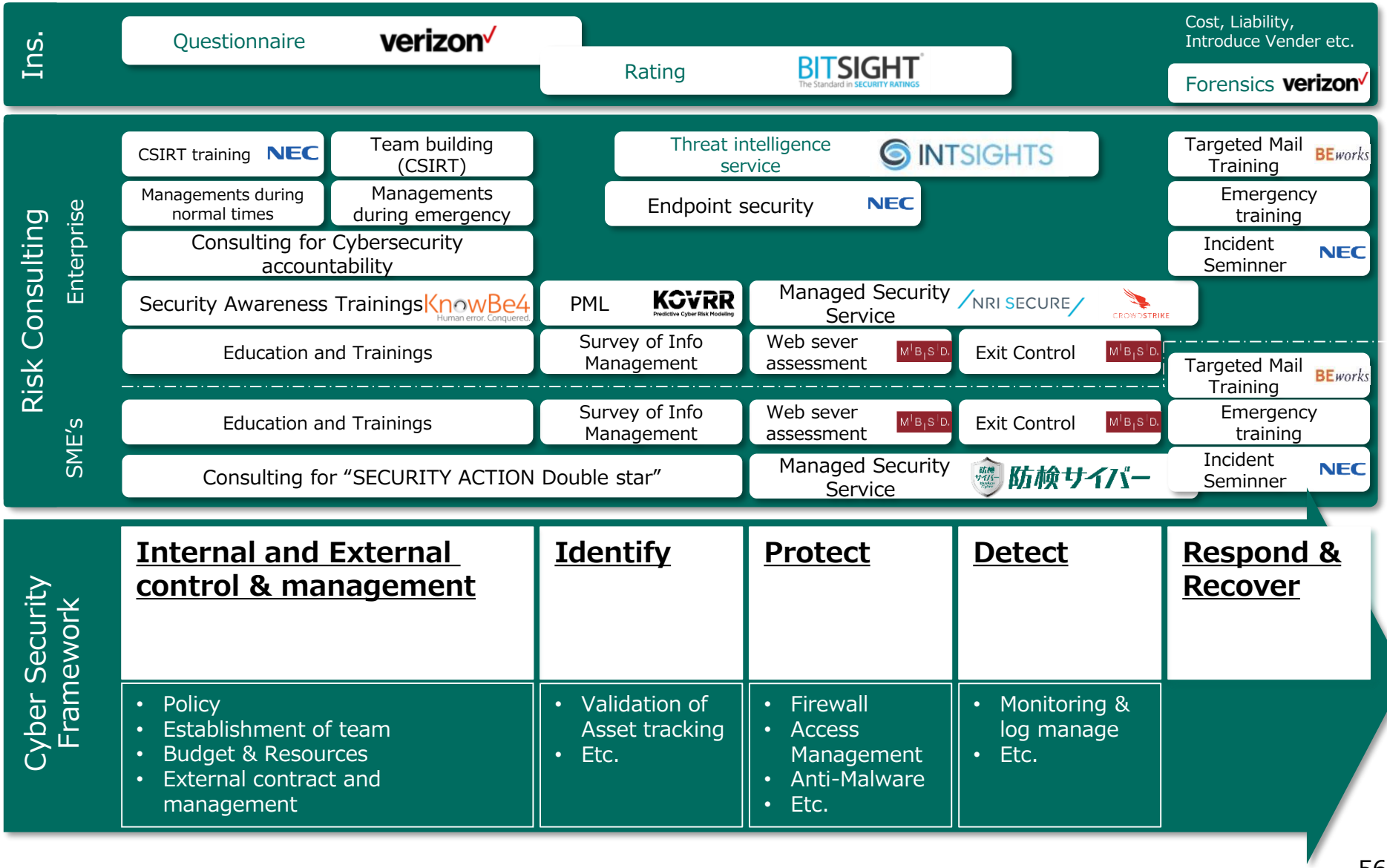
# Expectations for additional insurance services(3/3)

When the ancillary services that were selected as "necessary" were compared with the responses by cyber insurance status, the following results were obtained.Although the first three responses were the same, a higher percentage of companies without cyber insurance selected "security equipment with cyber insurance" and " Protection - detection - initial response to an incident package service " as "necessary ".
The services ranked first through fifth are particularly effective during response and initial response, suggesting that cyber insurance is required not only to compensate for damage caused by cyber accidents, but also to reduce such damage.

| Companies that do not have cyber insurance policy | | |
|---|---|---|
| Rank | necessary service | Rank (have cyber insurance policy) |
| 1 | Call center for consultation(56.7%) | 1 |
| 2 | ush services in case of accidents(47.1%) | 2 |
| 3 | Vulnerability assessment(30.8%) | 3 |
| 4 | security equipment with cyber insurance(24.6%) | 12 |
| 5 | Protection - detection - initial response to an incident package service(23.0%) | 6 |
| 6 | Security assessment (scoring) services(22.2%) | 5 |
| 7 | Service to calculate expected (maximum) damage(21.0%) | 7 |

# Cybersecurity MS&AD Platform

Advancing with you
MS&AD
INSURANCE GROUP



MS&AD

# MS&AD Insurance Group

MS&AD InterRisk Research & Consulting, Inc.
Cyber Risk Sec.

WATERRAS ANNEX, 2-105 Awaji-cho, Kanda,
Chiyoda-ku, Tokyo 101-0063, Japan
Tel : 03-5296-8961／Fax : 03-5296-8940
https://www.irric.co.jp/