

# Research of SMB's Cybersecurity measures in Japan 2020

**MS&AD** **MS&AD InterRisk Research & Consulting**

The number of cyber-attacks has been increasing year by year. In addition, the modus operandi and methods of attacks targeting companies and organizations are becoming more sophisticated and sophisticated, and there are cases of serious consequences. Cyber security is an important issue for companies and organizations, and if they fail to take appropriate measures and incur significant damages, they may be held liable for management and legal liabilities. In addition, the promotion of management reform and innovation using IT and the reform of work styles such as WFH, which many companies have started to implement, requires an ICT environment that can be used safely and securely, and cyber attacks threaten this premise.

In other words, it can be said that taking cyber security measures is an important issue that cannot be avoided in corporate management.

Every year, we conduct a survey on the current status and trends of corporate cyber security, including cyber security measures, damage status and issues, with the aim of contributing to the reduction of cyber security risks in the future. This year, we have added questions on security issues related to WFH (Work From Home) and other new normal ways of working, and the implementation status of measures.

We hope that this survey will help companies to take further action.

# Results and recommendations of this study

The actual situation revealed by this survey and the recommendations based on it are as follows.

① **Establishing a cyber security system is the first step of cyber security measures.**

Companies that have established a cyber security system (hereinafter referred to as "organizational system") have relatively better results in cyber security measures. The improvement activities are initiated by establishing an organizational structure.

② **Steady maintenance of documents and regulations**

In addition to the development of the organizational structure, it was also confirmed that it is important to develop the documents and regulations from policies (policies and action guidelines) to standards (standards and standards) to procedures (procedures) in a more practical manner in order to take security measures.

③ **Be aware of the cyber risks of the new normal way of working.**

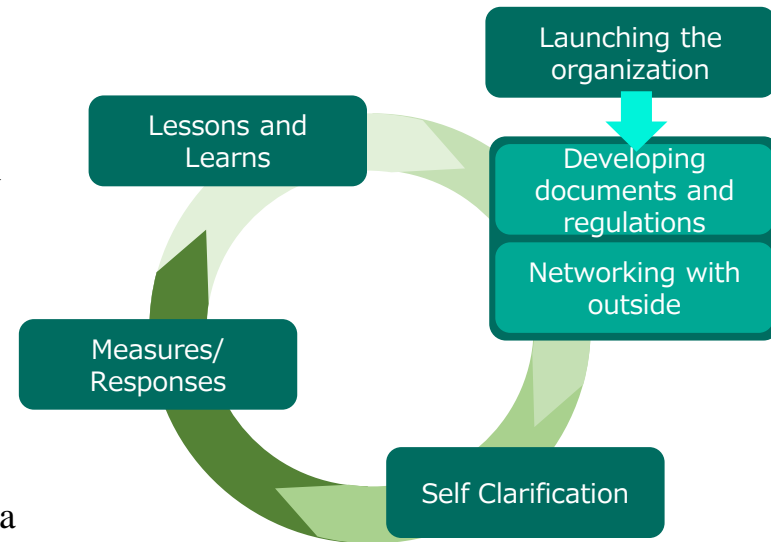
It was found that companies without an organizational structure were less likely to recognize the challenges of WFH and/or to review targeted e-mail training.

④ **Vulnerability management is handled by the organization based on the level of importance.**

Compared to the results of last year's survey, we found that vulnerability management in enterprises has not progressed. It is necessary to identify the vulnerabilities that truly need to be addressed and take efficient action.

⑤ **Consider the need for insurance, including additional services.**

Although the participation rate of cyber insurance is still not high, the results show that the awareness of cyber insurance itself is gradually increasing. In addition, many companies that do not have cyber insurance cited "a package service that covers protection, detection, and initial response in case of an incident" as an expected supplementary service. It is recommended to consider the necessity of cyber insurance as well as supplementary services.



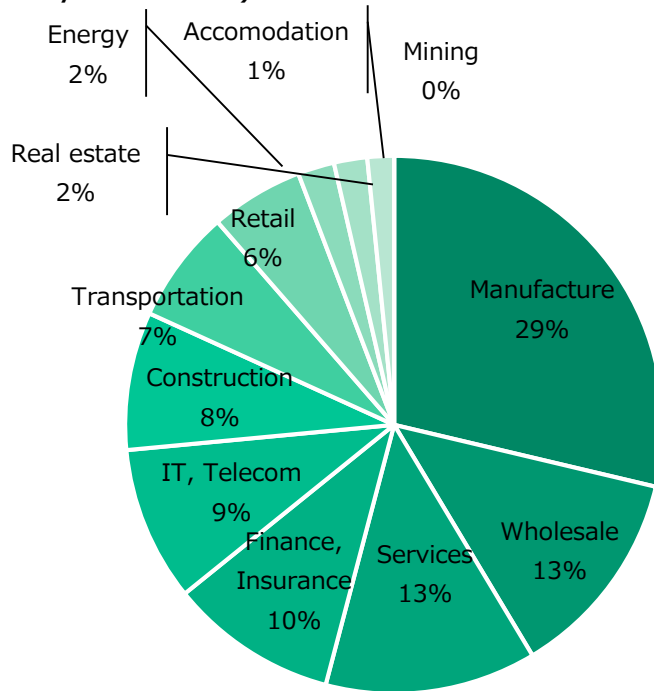
# Survey Summary

## Outline of Research

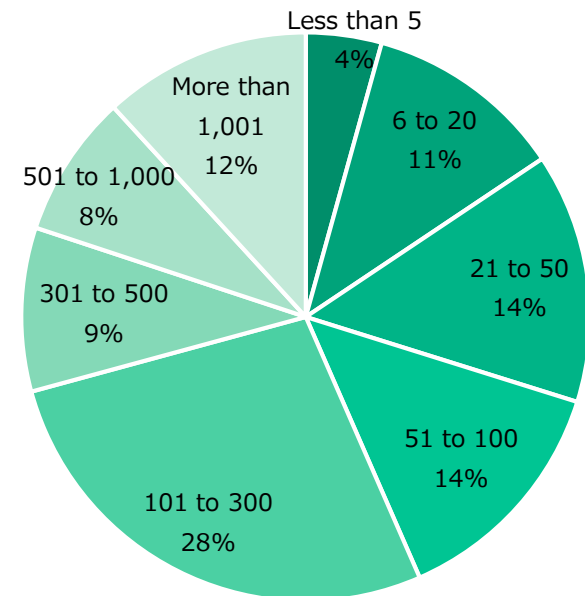
Survey Method	Mailing Questionnaire (combined with web-based response)
Target companies	<u>10,000 companies</u> in Japan Extracted from Toyo Keizai Inc.'s "40,000 company data in Japan ((1) Basic data)" Companies that randomly extracted in industry by industry
Number of valid responses	557 (total collected number: 563) Recovery rate <u>5.5%</u>
Survey period	November 18 - December 4, 2020.

## Industry and size of responding companies

Industry (n=557)



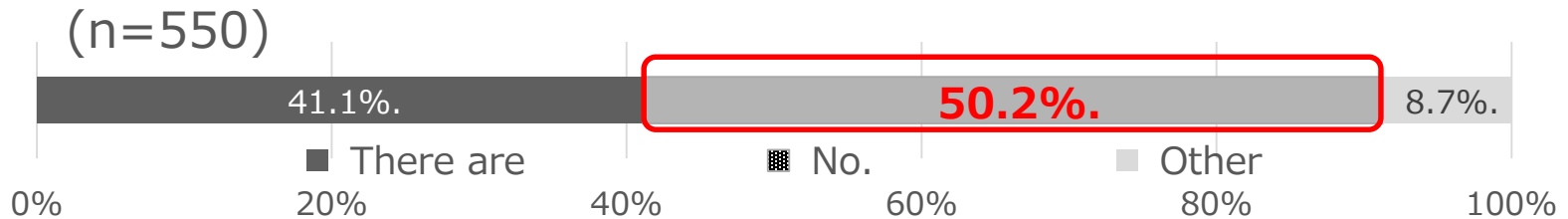
Number of employees (n=557)



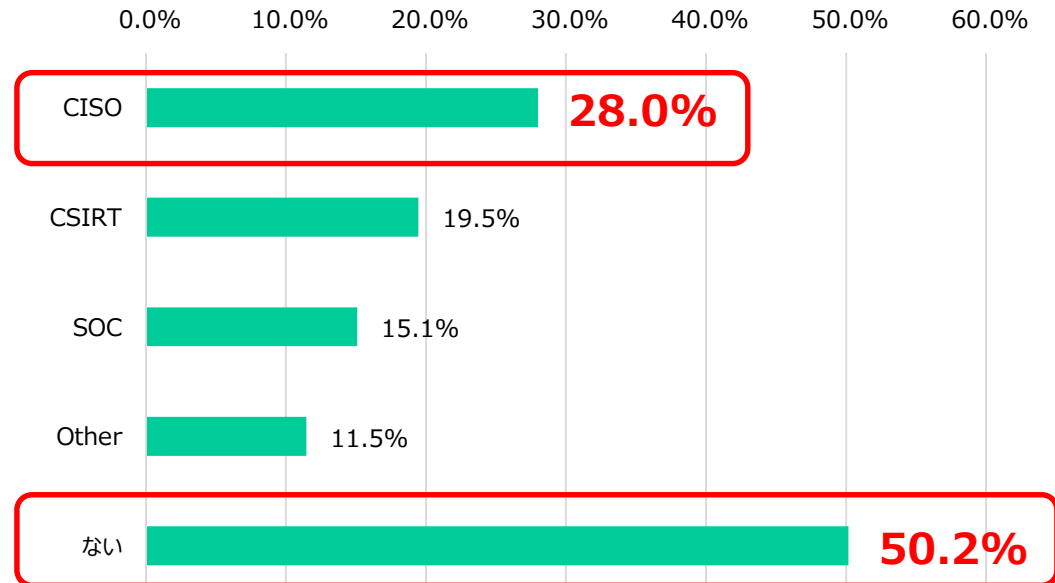
## Internal management system

## Cyber security system in place\* Multiple choices (1/2)

Half of the respondent companies had not established a cyber security system, and among the companies that answered that they had a cyber security system, "CISO" was the most commonly established.



CISO	<p>Chief Information Security Officer                      A position that oversees and manages the organization's information security. Its main roles are to formulate security policies, lead the response to security incidents, bridge information security-related issues to the management, and manage information security within the organization.</p>
CSIRT	<p>Computer Security Incident Response Team                      An organization that responds to cyber security-related incidents such as information leaks and system failures caused by cyber attacks. It also conducts research and other activities during normal times, not just during incidents (emergencies).</p>
SOC	<p>Security Operation Center                      An organization that monitors and analyzes the logs generated by information security devices, servers, and computer networks to detect and notify cyber attacks. There are two types of SOC: those that monitor their own organizations and those that provide services to monitor their customers.</p>



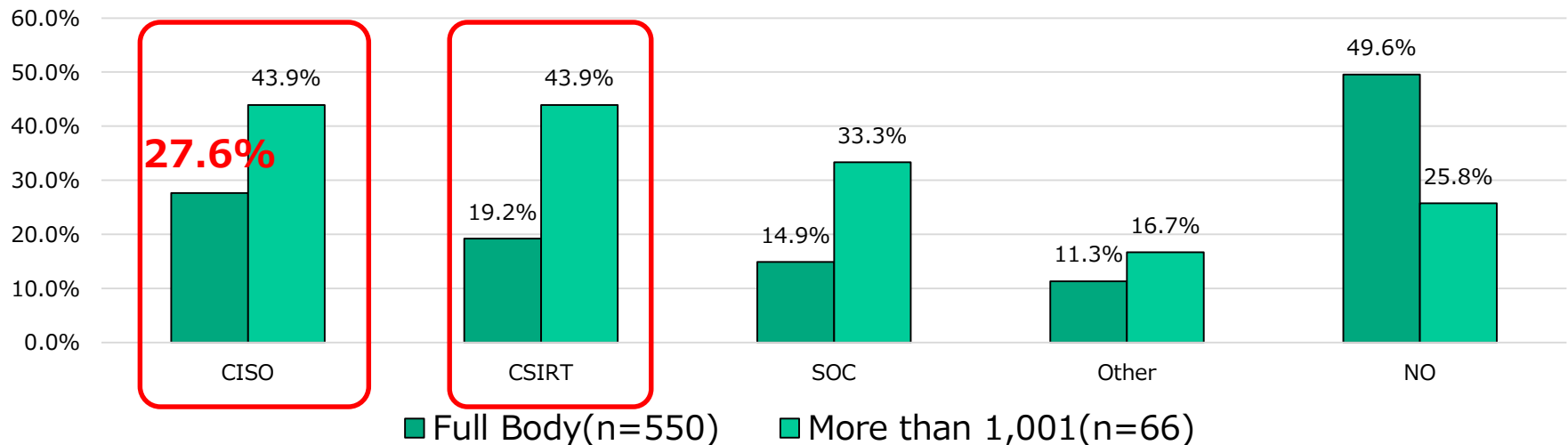


## Cyber security system in place\* Multiple choices (2/2)

Furthermore, by the number of employees, "CSIRT" and "SOC" (43.9% each) were established most frequently in companies with **1,000 or more employees**, suggesting that company size (employee size) is related to the establishment of organizational systems. In addition, "PSIRT" was mentioned for the first time since the start of this survey in companies that selected "Other".

The reasons given by companies that chose "no" were lack of human resources, lack of knowledge and skills, and lack of understanding on the part of management.

PSIRT	Product Security Incident Response Team An organization that addresses the risks arising from vulnerabilities in the products offered by the organization. Conducts activities to address vulnerabilities in its products and to manage and improve the security quality of its products.
-------	--

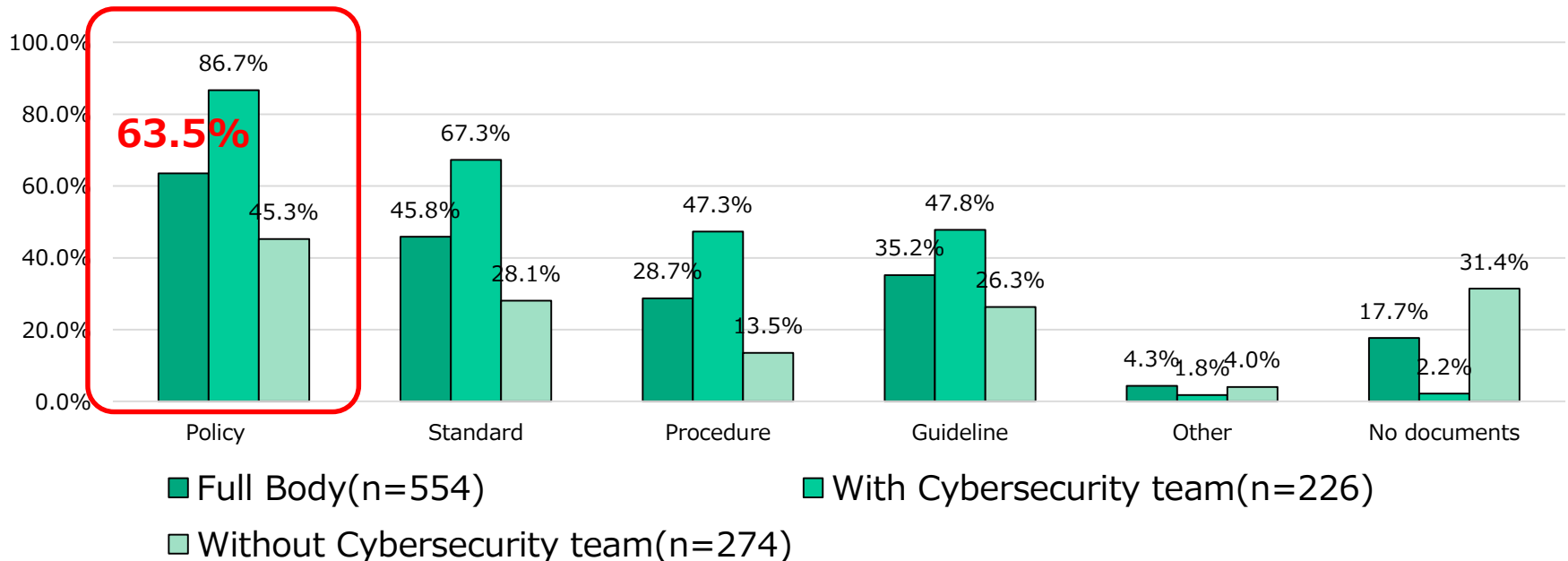


## Documents and regulations related to security that are in place\*

### Multiple choices (1/2)

The most common document/regulation related to security was the "Policy" (63.5%). Overall, there was a difference depending on the existence of organizational structure. For companies that selected "Other," "In line with the rules of the group company/parent company/head office" and "Included in the company rules such as employment regulations" were the most common responses.

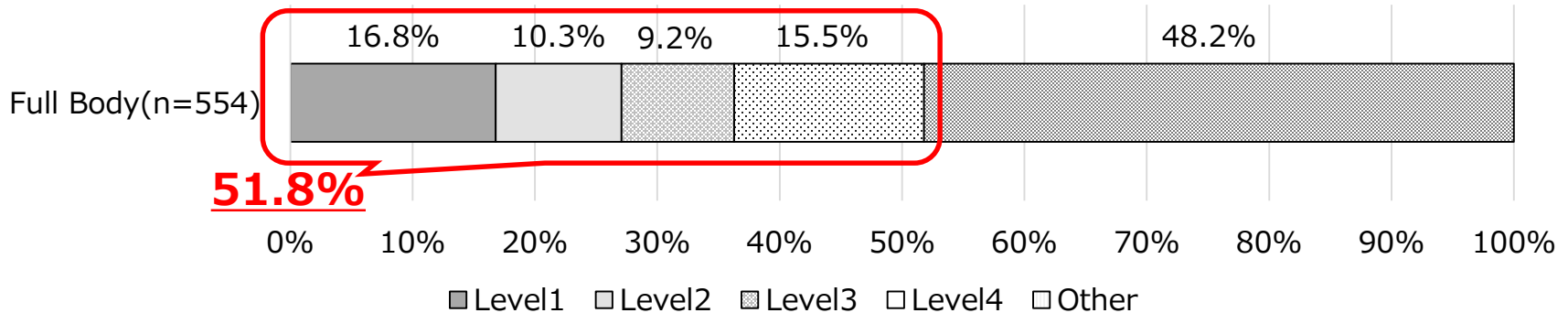
The reasons given by companies that chose "no" included "lack of knowledge" and "lack of human resources."



## Documents and regulations related to security that are in place\*

### Multiple choices (2/2)

The status of security-related documents and regulations was categorized into five levels, as shown below, assuming that they are developed from policies to standards to procedures to guidelines.

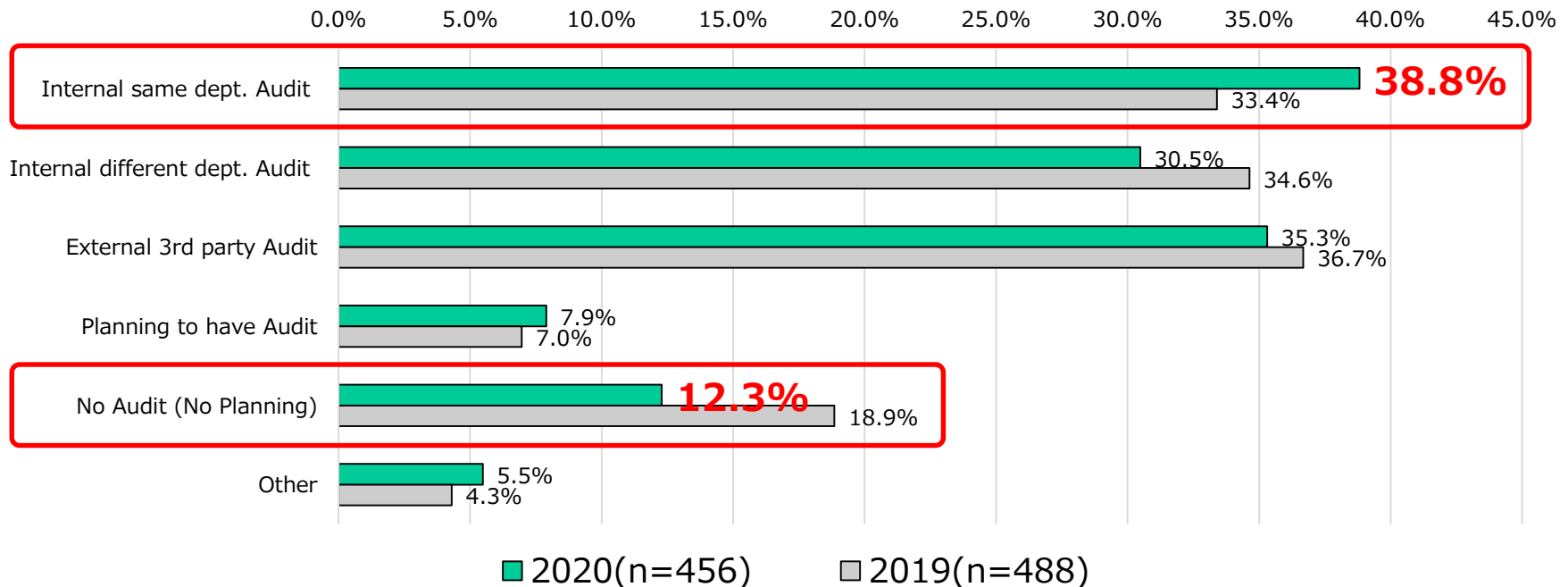


	Policy	standard	Procedure	Guidelines
Level 1	Done	N/A	N/A	N/A
Level 2	Done	Done	N/A	N/A
Level 3	Done	Done	Done	N/A
Level 4	Done	Done	Done	Done
Other	All items that do not fall under Levels 1 through 4			

## Whether or not the described contents are implemented/audited.

(Only if you answered "Yes" to the previous question)

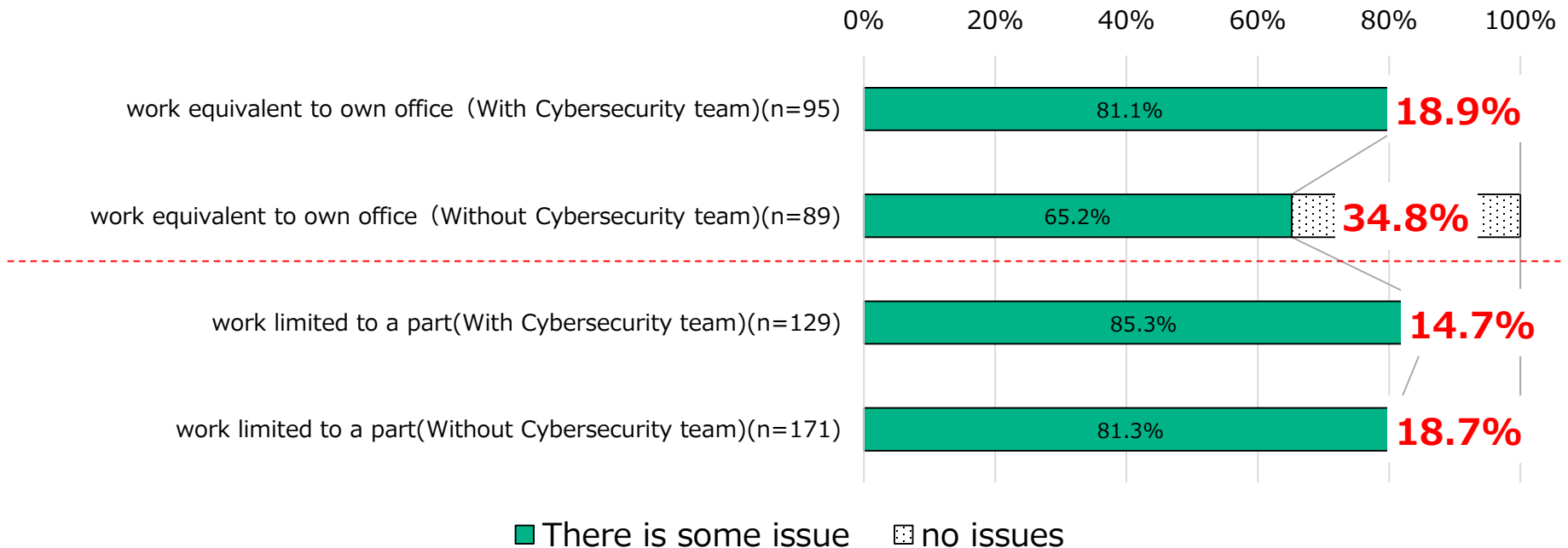
Of the companies that responded that they have documents and regulations, we asked whether they check or audit whether the contents described in the documents and regulations regarding security are being implemented. The most common answer (**38.8%**) was "Internal same dept. Audit". Compared to the last year's survey, the number of respondents who answered "No Audit(no planning)" decreased, suggesting that the system has been improved.



## Challenges in implementing WFH\* Multiple choices

We surveyed the challenges of WFH by type of WFH implementation ("work equivalent to own office" and "work limited to a part"). When we checked the responses by the existence of an organizational structure, a higher percentage of companies without an organizational structure responded that there were "no issues" than companies with an organizational structure in any WFH format.

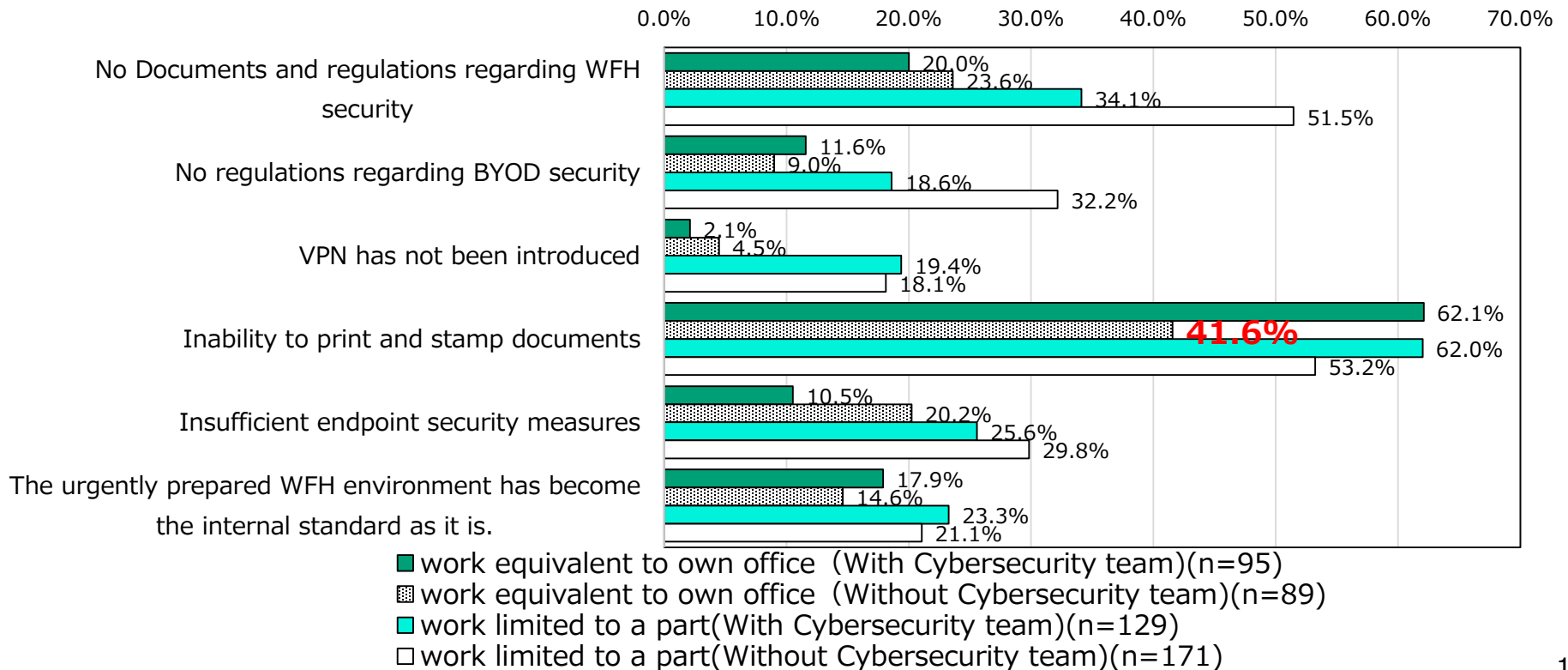
**In situations where control by the organization is not sufficient, it is possible that "issues are not recognized as issues."**



## Challenges in implementing WFH\* Multiple choices

When the issues were checked in detail, the number of companies without an organizational structure was lower than that of companies with an organizational structure for "Inability to print and stamp documents".

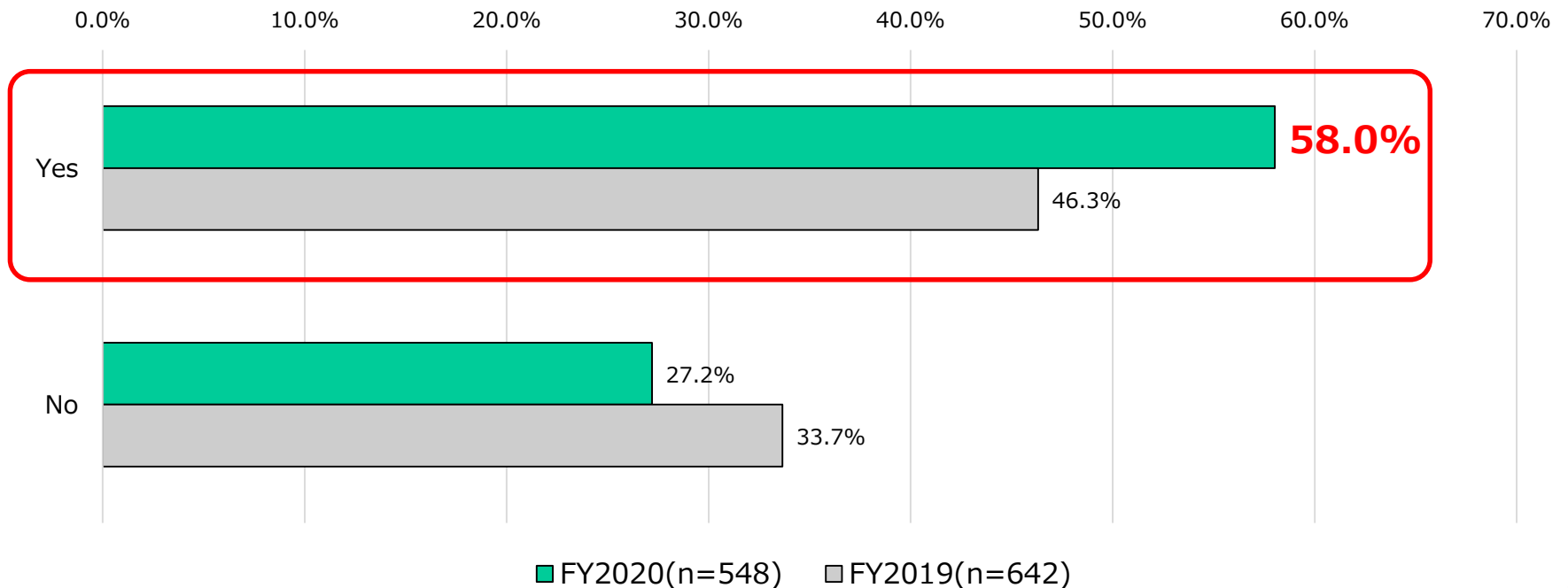
**Conducting business without adequate controls and without recognizing risks can increase the possibility of information leaks. It is once again important to establish an organizational structure to resolve the issues.**



**External management system**

## Implementation status of security assessment and evaluation for selecting cloud service providers (1/2)

We checked whether or not security is evaluated when selecting a cloud service provider. Compared to the last year's survey, the percentage of respondents who answered "yes" to the question increased. One reason may be that WFH and other factors have necessitated the migration of internal assets to cloud services, and each company has established a system to conduct evaluations.

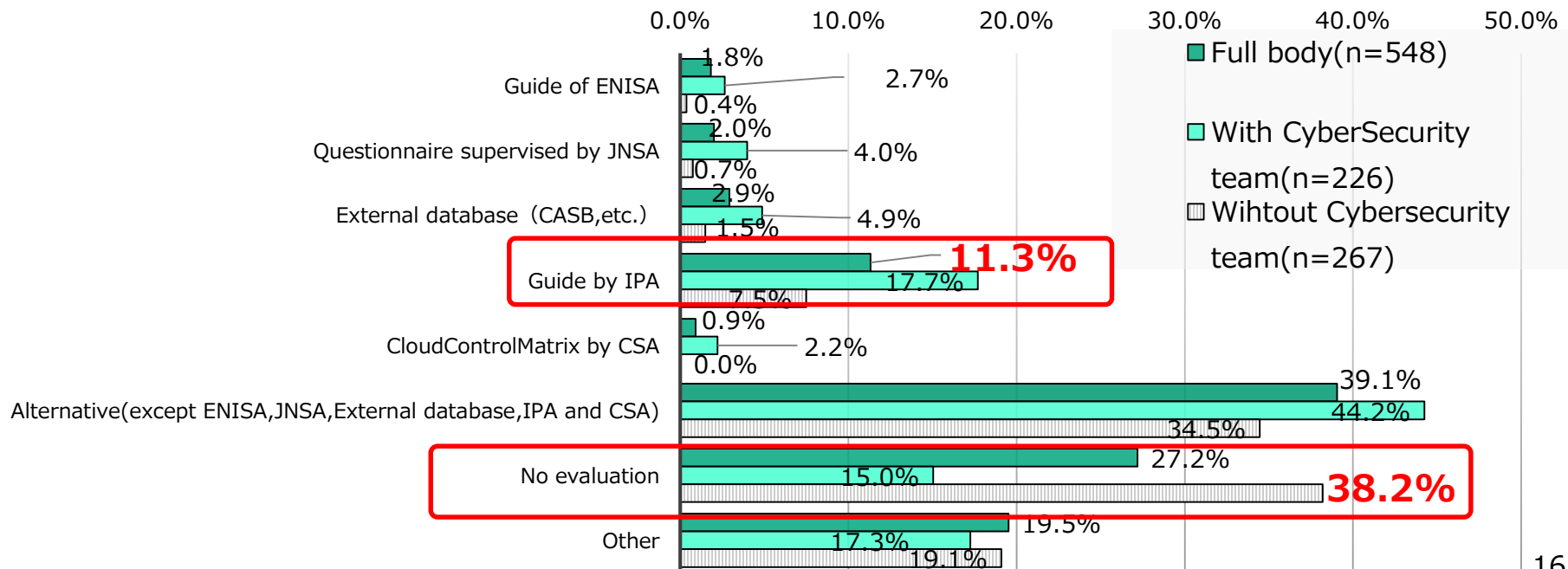




## Implementation status of security assessment and evaluation for selecting cloud service providers (2/2)

Guide by IPA was the most common choice in the questionnaire (11.3%), regardless of whether there was an organizational structure, while "No evaluation" was the most common choice (38.2%) among companies without an organizational structure.

**It was confirmed and is expected that the security measures for the use of cloud services, which will be increasingly expanded in the future, will be "modeled as a recommended system configuration including cloud services that enterprises can use with confidence" based on policies and demonstrations.**



**Identify**

## Status of handling of information assets in possession

We asked the respondents whether they categorized the scope of information disclosure for the information assets they possess (e.g., information that should be kept confidential, information that is limited to internal use, information that can be provided to parties with whom they have concluded nondisclosure agreements, and information that can be made public). The overall response status is shown in the table below.

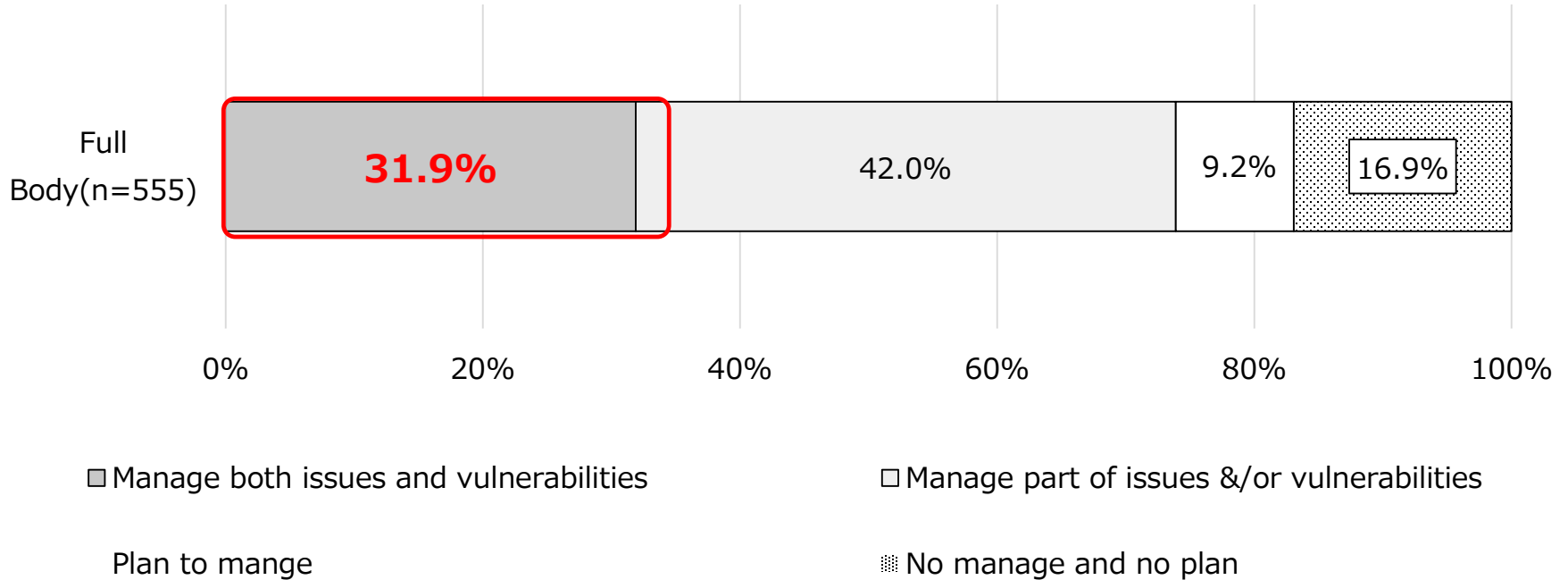
Although the largest number of companies (**46.8%**) answered that they "have journal rules (documented) and classify according to those rules" (option 1.), less than half of the companies were able to do so.

		Classify Information assets		Not classify Information assets	
Documented Rules	Have	1. Executing <b>(46.8%)</b>	2. Not Executing (6.6%)		
	Not have	3. Planned to be documented (2.0%)	4. Not planned to be documented (8.2%)		

## Issues and vulnerabilities of information assets held (1/2)

(e.g., keeping confidential information where anyone can see it, not encrypting passwords, etc.)

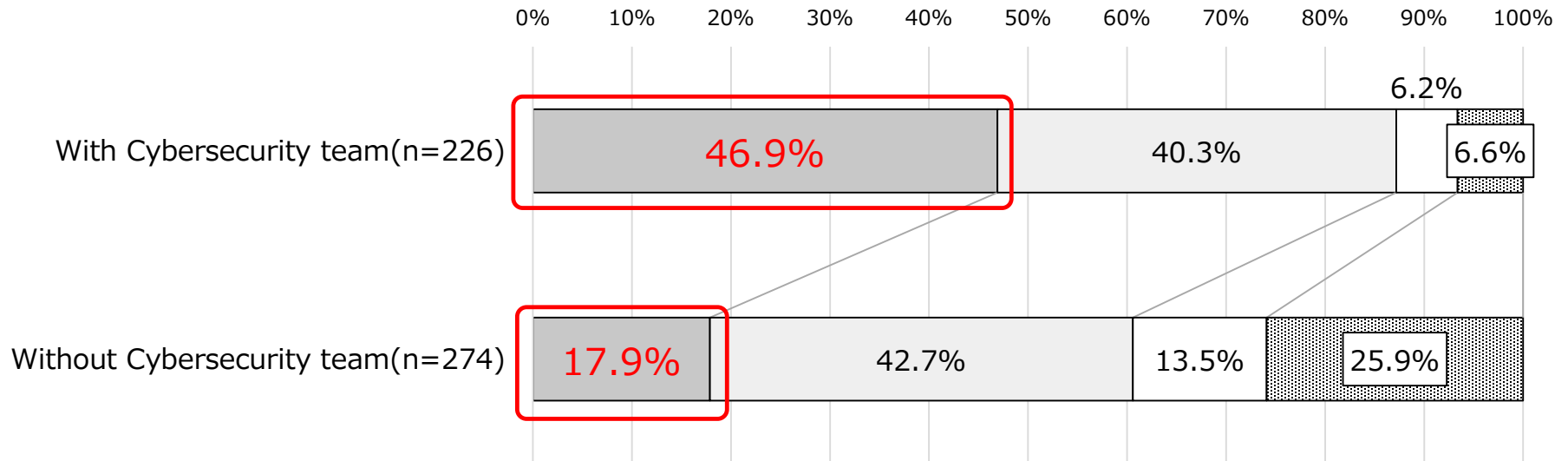
We asked about the status of the management of issues and vulnerabilities of the information assets they own. Overall, only 31.9% of the respondents answered that they are managing both issues and vulnerabilities.



## Issues and vulnerabilities of information assets held (2/2)

(e.g., keeping confidential information where anyone can see it, not encrypting passwords, etc.)

When this question is broken down by the presence or absence of a corporate cyber security team, **46.9% of the companies** with Cybersecurity team answered that they “manage both issues and vulnerabilities,” while only **17.9% of the companies** without a team, indicating a large difference depending on the presence or absence of a system.



- Manage both issues and vulnerabilities
- Plan to manage

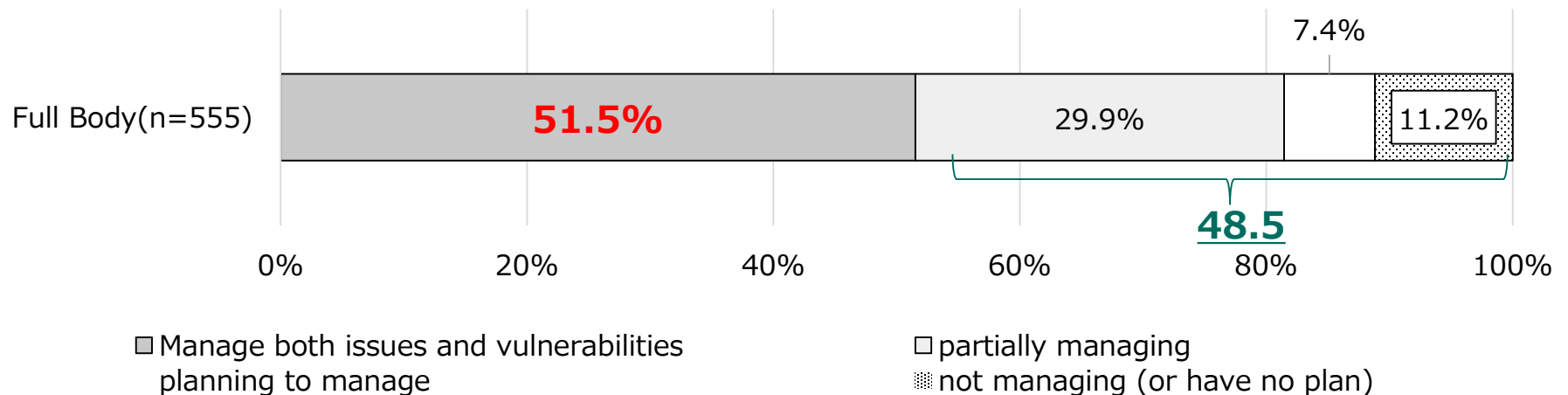
- Manage part of issues &/or vulnerabilities
- No manage and no plan

## Challenges and vulnerabilities in hardware asset management of owned IT devices (1/2)

(e.g., not knowing where and by whom deployed PCs are managed, and not realizing that PCs are lost)

We checked the issues in hardware asset management of IT devices and the status of vulnerability management.

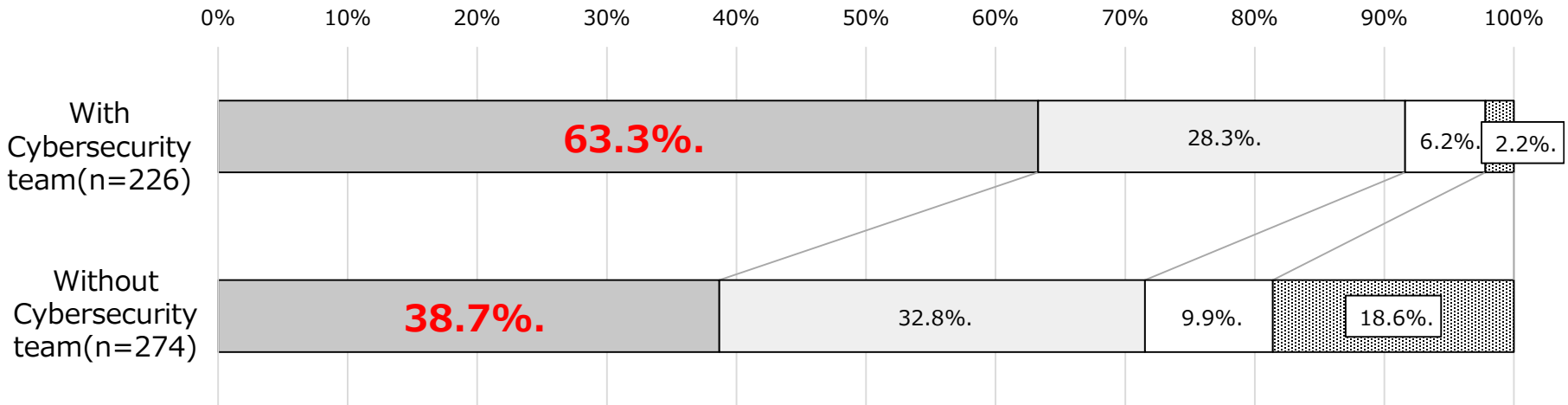
Overall, 51.5% of the respondents answered that they are managing both issues and vulnerabilities, but nearly half (48.5%) of the total respondents answered that they are "partially managing", "planning to manage", and "not managing (or have no plan)". This indicates that nearly half of the companies (48.5%) are not sufficiently managing vulnerabilities.



## Issues and vulnerabilities in hardware asset management of owned IT devices (2/2)

(e.g., not knowing where and by whom deployed PCs are managed, and not realizing that PCs are lost)

When this question was divided into the presence or absence of a corporate cyber security system, **63.3% of** the companies with a cyber security system answered "managed" while **38.7% of** the companies without a system, showing a large difference depending on the presence or absence of a system.

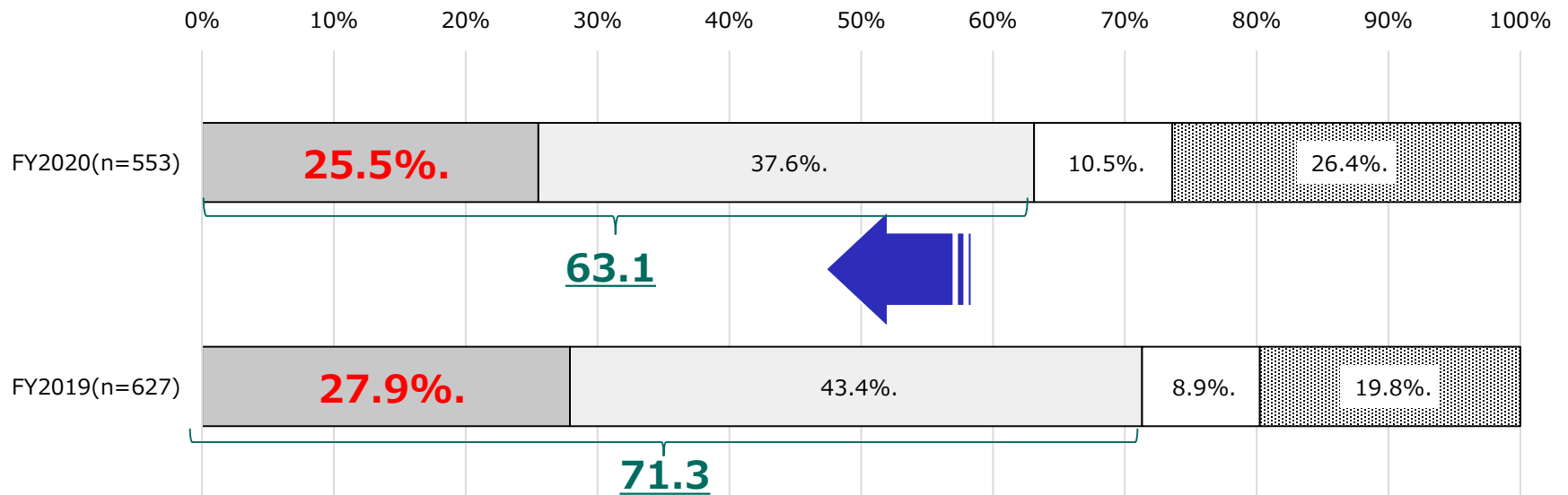


- Issues and vulnerabilities are managed.
- Some of the issues/vulnerabilities are managed.
- Planning to manage issues/vulnerabilities
- No issues/vulnerabilities are managed (no plan)

## Management status for vulnerabilities (1/2)

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

We asked the respondents whether they manage the vulnerability of PCs and software. **More than 70% of the** companies had a documented management system in place last year, but this year, the figure was less than 70%. In addition, **less than 30%** of the companies have documented their practices.



- The management method is defined (documented) and implemented.
- Partially implemented.
- Have a plan to manage it in the future.
- Not managed (and no plan)

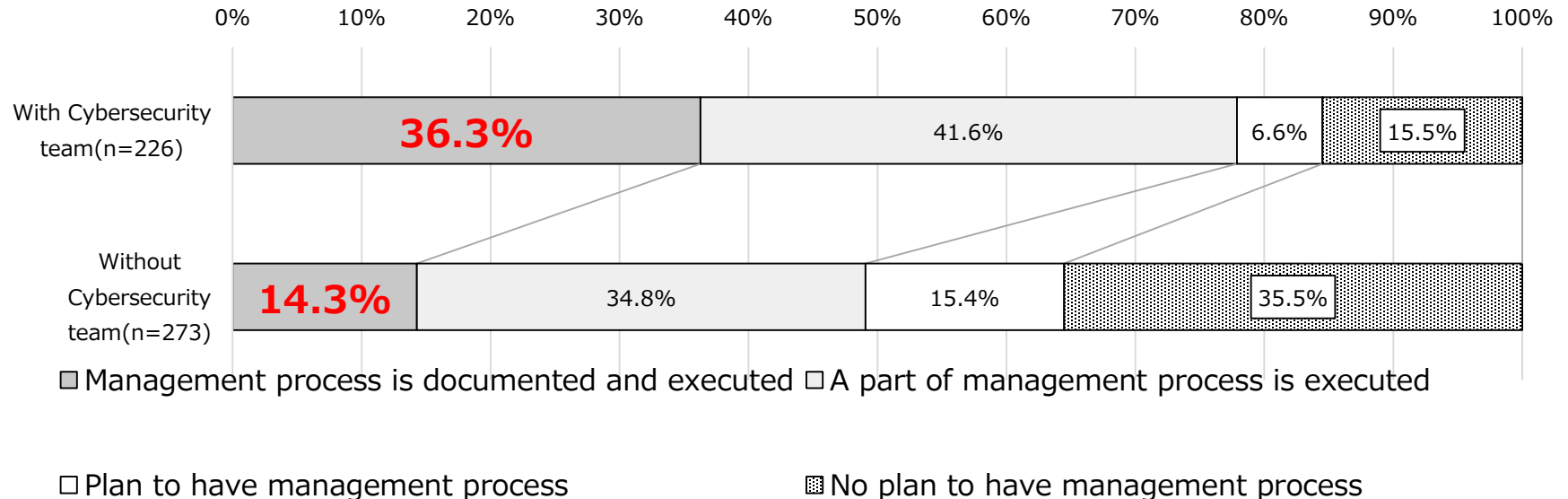


## Management status for vulnerabilities (2/2)

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

In terms of the presence or absence of a cyber security system, **36.3% of** companies with Cybersecurity team responded that "Management process is documented and executed" while only **14.3% of** companies without a Cybersecurity team responded that same answer.

New vulnerabilities are being discovered every day, and there are cases of cyber-attack exploitation. It is necessary to determine the priority of the response, including the known vulnerabilities, and to respond effectively as an organization.



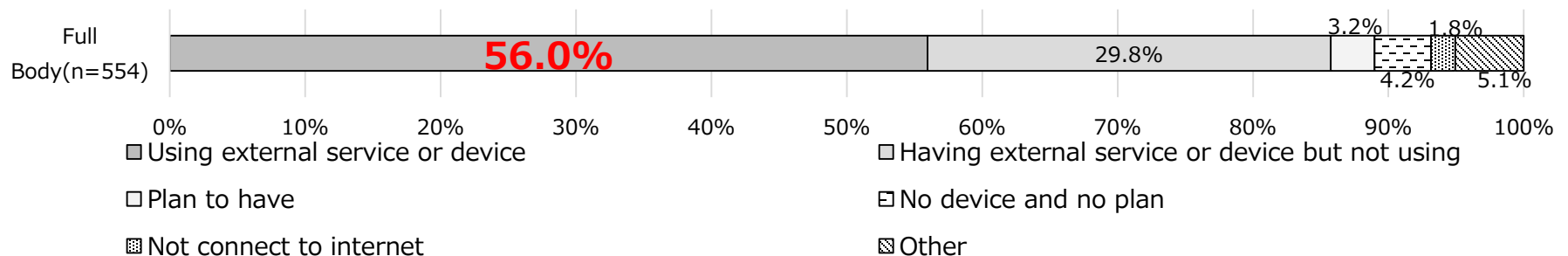
**Protect**

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

We checked the implementation status of perimeter protection between the Internet and the company's network. Overall, **56.0%** of companies **Using external service or device**.

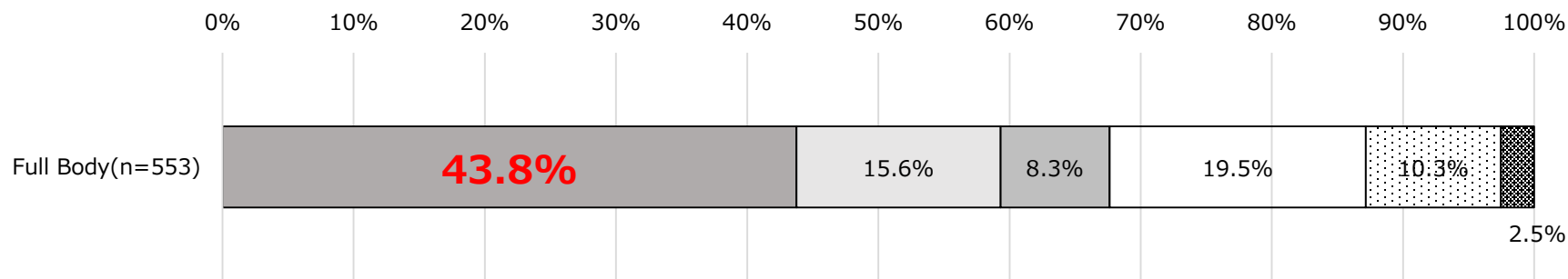
On the other hand, **29.8%** of the companies said they have purchased but have not been able to using it, which means that the effectiveness of the security measures remains an issue, as they cannot immediately respond to cyber attacks or fully demonstrate their effectiveness.

In addition, in the “Cyber Security Rangers” that we were selected by IPA, there were cases where the staff didn’t realized about installed UTMs. We believe that a one-stop security service that provides monitoring and incident response services is necessary for companies that cannot devote resources to their own operations.



# Establishing rules for user IDs, passwords, and permissions to view and update information (1/2)

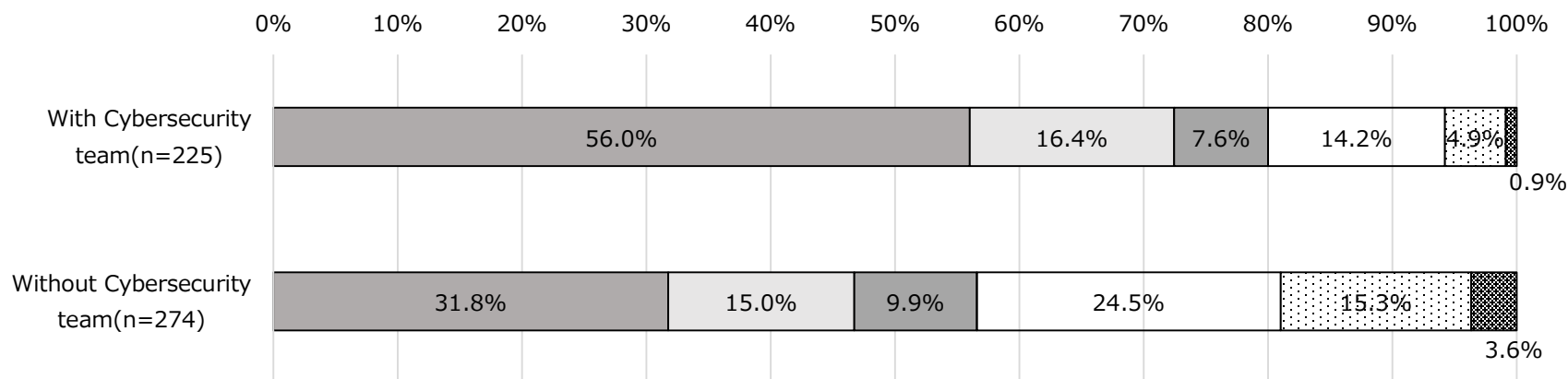
Overall, about half (**43.8%**) of the companies responded that "rules regarding IDs, passwords, and information access updates are documented, checked, and reviewed. In addition, "Other" includes "No rules, but inspections are carried out," "Depends on/complies with the parent company," and "Only PCs that handle personal information are inspected. " and "Only PCs that handle personal information are inspected."



- Documented Rules and check, review process.
- Documented Rules and but not check, not review process.
- Plan to document rules
- Has rules but not documented
- No rules and no plan
- Other

# Formulate rules for user IDs, passwords, and permissions for referencing and updating information (2/2)

Answer “percentage of” companies with Cybersecurity team was **56.0%**, while the percentage of companies without a cyber security structure was **31.8%**.



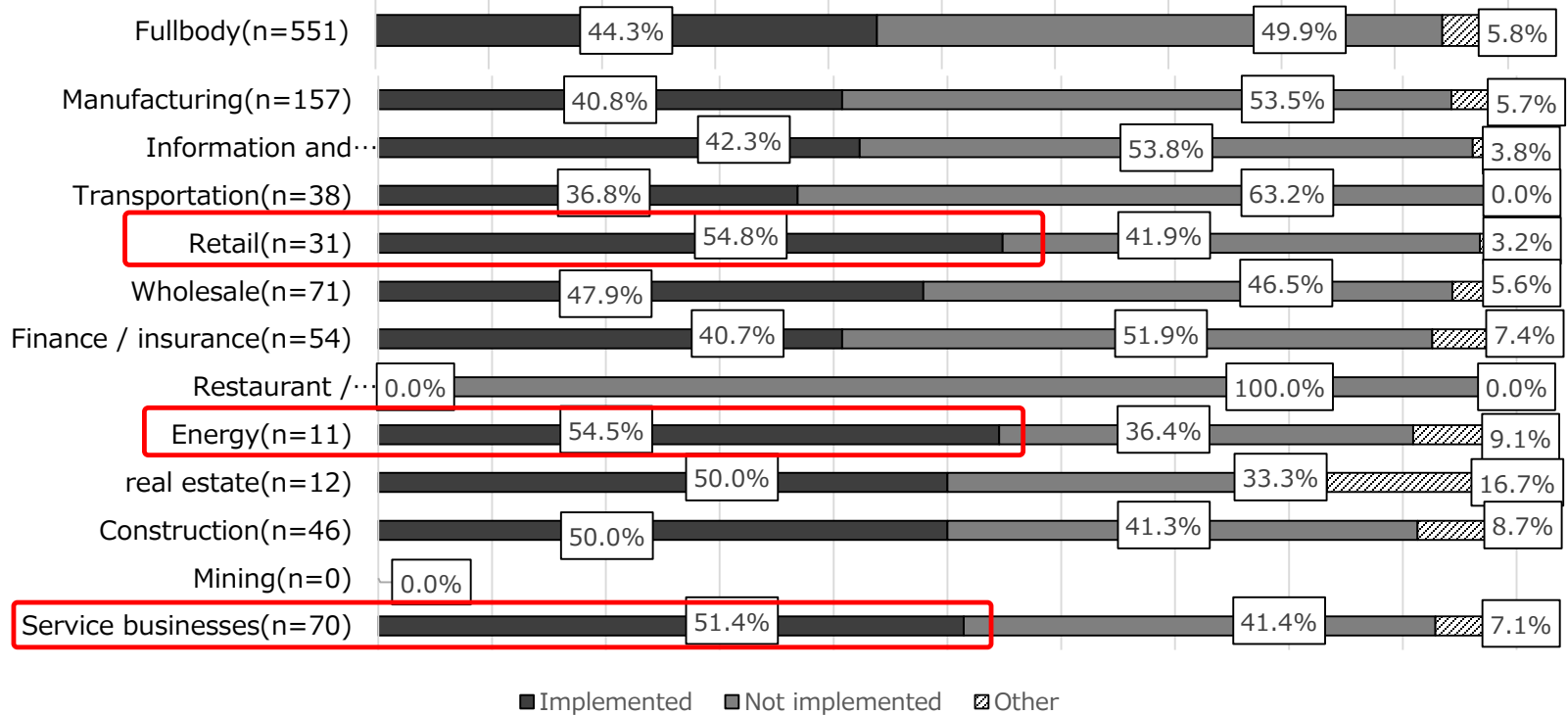
- Documented Rules and check, review process.
- Documented Rules and but not check, not review process.
- Plan to document rules
- Has rules but not documented
- No rules and no plan
- Other

**Detect**

# Implementing EDR (Endpoint Detection and Response)

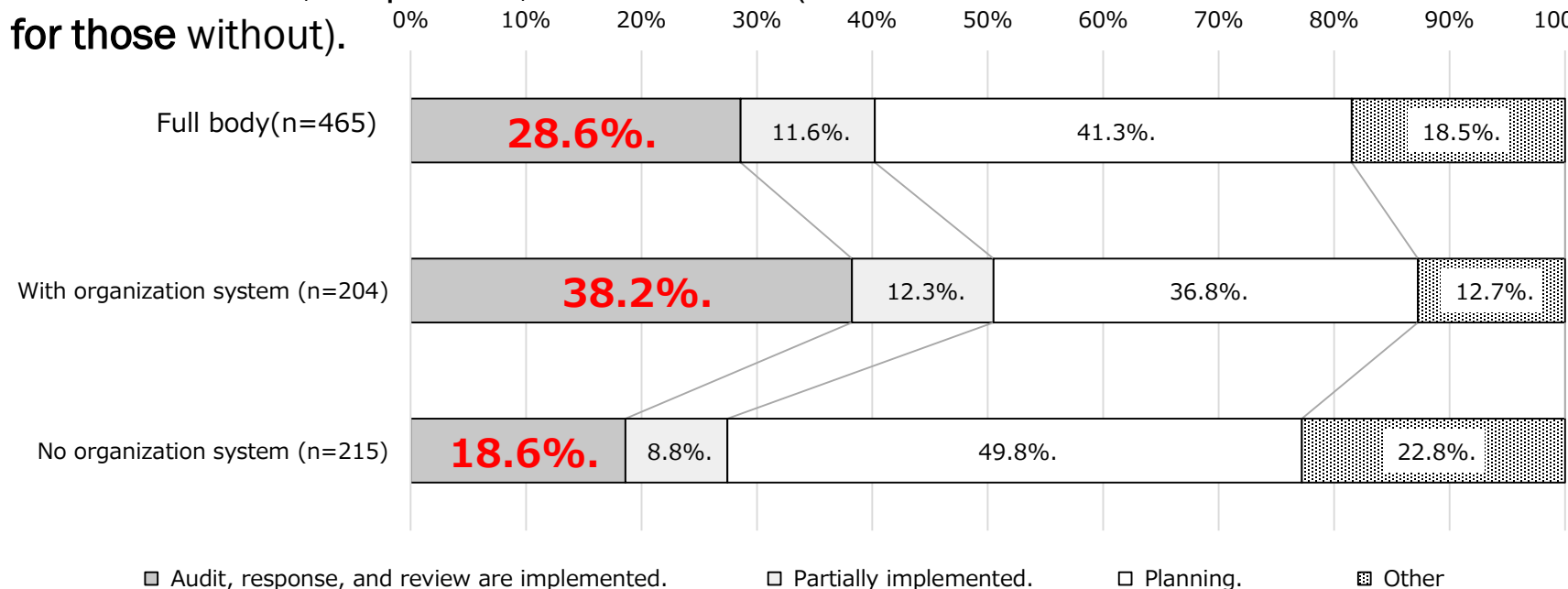
For the status of EDR (Endpoint Detection and Response) implementation, please refer to Among companies that responded, "Implemented", the **retail industry (54.8%)**, followed by the **energy industry (54.5%)** and **other service businesses (51.4%)** came out on top.

The measures are being taken by companies that handle PII and IP information.



## Whether the security monitoring system's process for responding to and responding to security alerts has been reviewed

We asked the respondents whether they responded to security alerts generated by security monitoring systems (IPS, IDS, etc.) and whether they reviewed their response processes. Overall, only **28.6% of the** companies answered that they "audit, respond to, and review security alerts," indicating that they are not fully prepared. The same trend was observed for companies with and without an organizational structure, but there was a nearly double difference in the percentage of companies that answered that they "conduct audits, responses, and reviews" (**38.2%** for those with a structure and **18.6%** for those without).

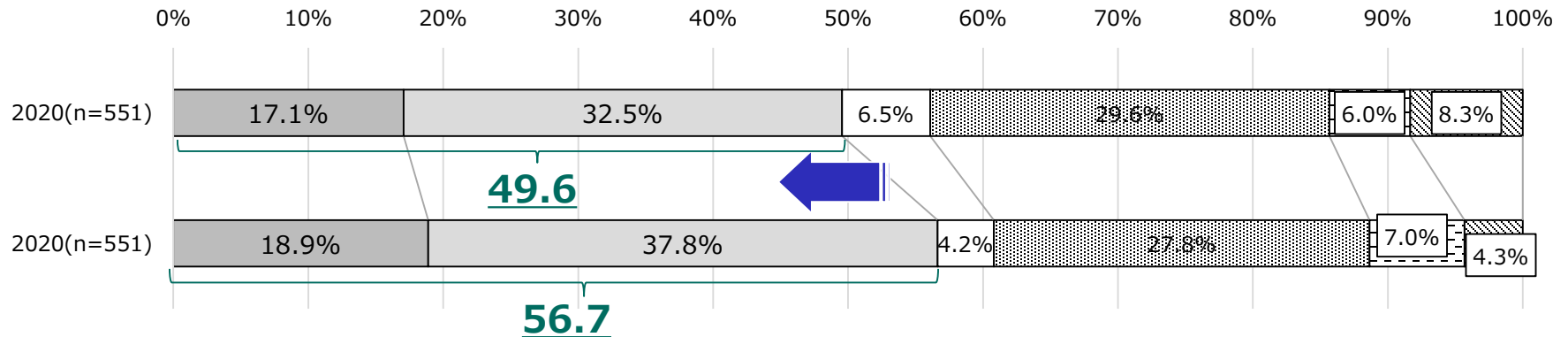




# Contracts for emergency support services, etc. in the event of a security incident (accident)

Compared to the previous year, there was no significant change in the overall response rate trend, but the percentages of "I have a contract with an emergency response service in case of an incident" and "Emergency response is conducted in-house" decreased.

With limited budgets and personnel, there is a possibility that the resources available for contingency planning are decreasing. Under such circumstances, there is a great deal of room for proactive use of services such as referrals to specialized service providers attached to cyber insurance in the event of an accident.



- ☐ I have a contract with an emergency response service in case of an incident
- ☐ Emergency response is conducted in-house
- ☐ Emergency response service contracts are planned in the event of an incident
- ▣ No contract and plan
- ☐ Planning of contracting emergency support services to respond to incidents when they occur

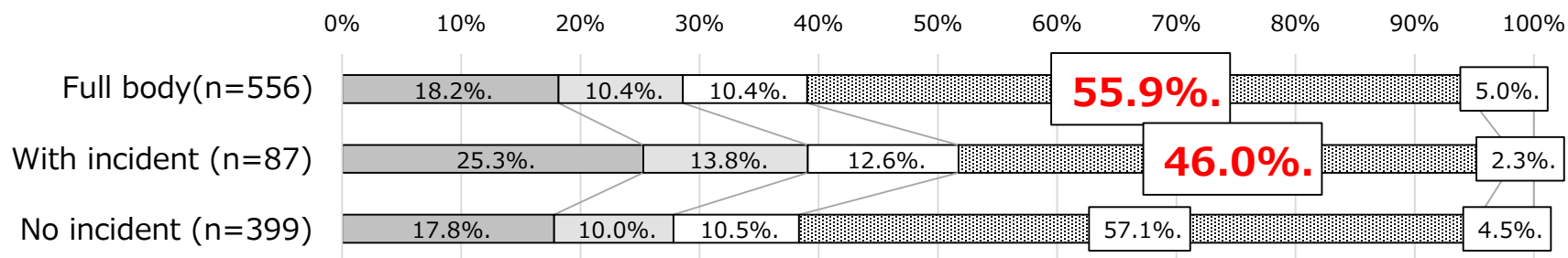
**Respond and Recover**

## Status of training for security incidents (1/2)

As for whether they conduct drills in case of security incidents (accidents), the majority (**55.9%**) of the total companies answered that they do not conduct drills (nor do they have plans to do so).

Other" included "Same as parent company," "Implemented by each department," and "Only education (classroom).

While a larger percentage of companies with experience of cyber security incidents responded that they "conduct training" than those without experience, there are **more than 40%** of companies that "do not conduct (nor plan to conduct) training" despite their experience of incidents. It is necessary to enhance the training menu.

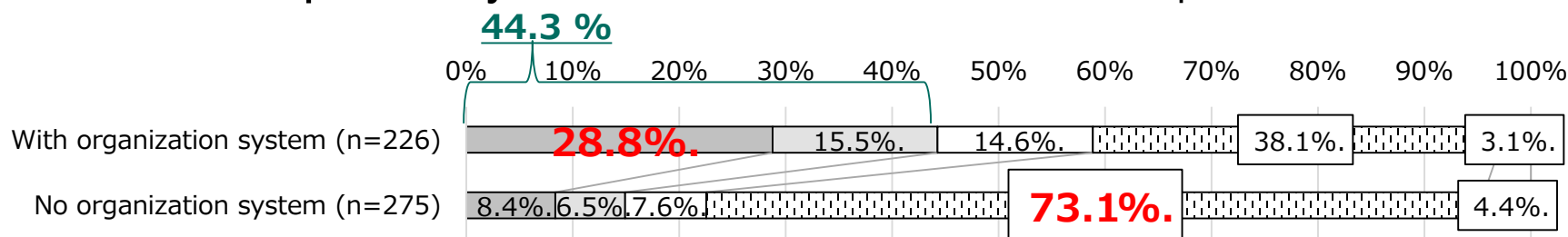


- Training is conducted (non-IT departments also participate)
- Training is being conducted (IT department only)
- Training is planned.
- No training is conducted (no plan)
- Other

## Status of training for security incidents (2/2)

Among companies with an organizational structure, many companies (28.8%) answered that they "conduct training," and if "only the IT department conducts training" is included, it accounts for about 40%. On the other hand, more than 70% (73.1%) of the companies without an organizational structure answered that they "do not conduct training."

For companies with an established organizational structure, security incident response can be carried out while making appropriate decisions and responses as an organization and utilizing past experience. For companies without an organizational structure or with a small number of employees, it is necessary to outsource functions that can handle possible cyber-attacks at the time when the scope of influence is small.



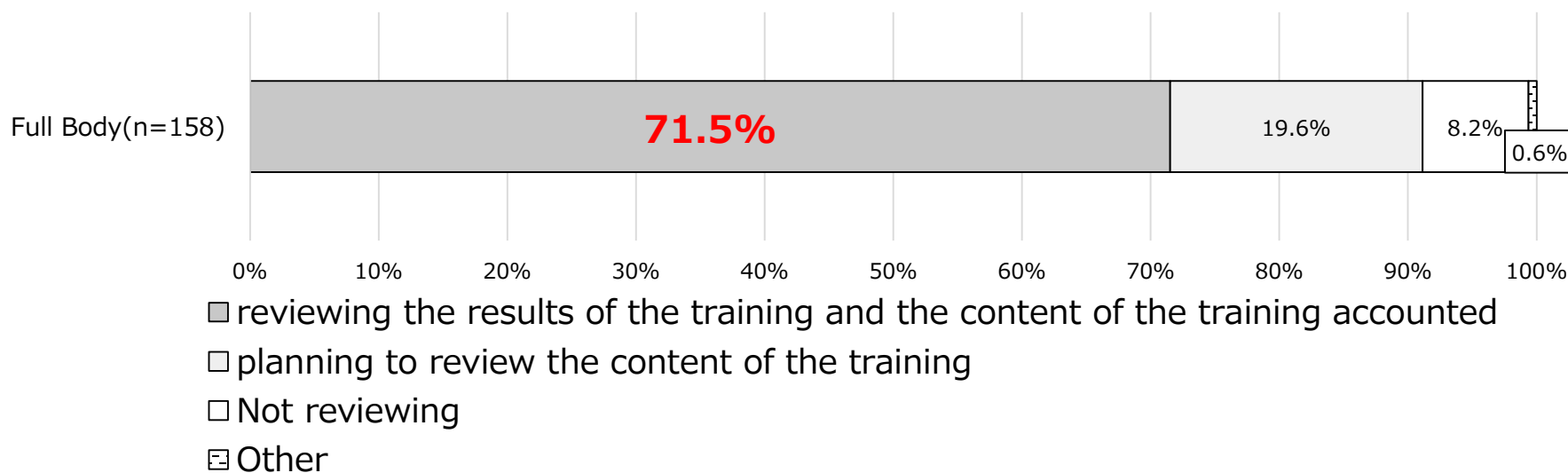
- Training is conducted (non-IT departments also participate)
- Training is being conducted (IT department only)
- Training is planned.
- No training is conducted (no plan)
- Other

## Whether the results of security incident training are reviewed

(If you answered "1. Training is conducted (non-IT departments also participate)" or "Training is conducted (IT departments only)" in the previous question)

The companies that are currently reviewing the results of the training and the content of the training accounted for **71.5%** of the total, and when the companies that are planning to review the content of the training (**19.6%**) are included, the companies that are reviewing/plan to review the content account for **about 90%** of the total.

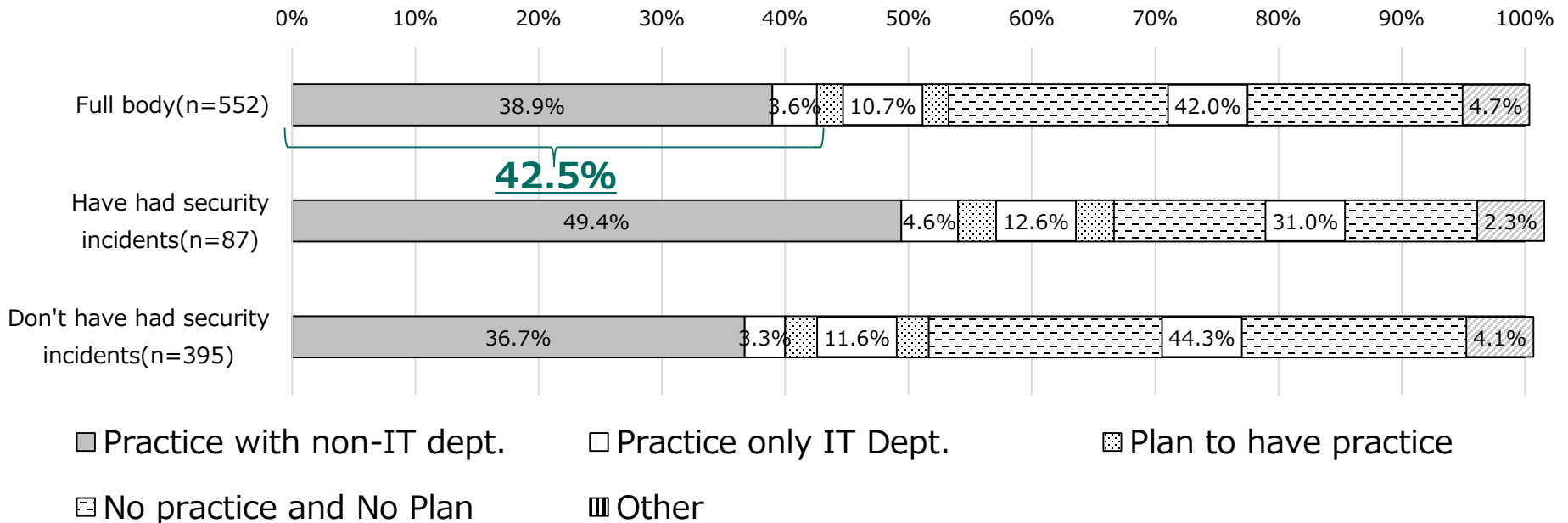
The "Others" category included responses such as "Will be handled by the parent company" and "Do not feel the need to review."



## Training for incoming suspicious emails (targeted email training) (1/2)

Regarding whether companies are conducting training for incoming suspicious e-mails (targeted e-mail training), **42.5% of the** total companies answered that they are conducting training (total number of Practice with non-IT dept. and practice only IT dept). If "planning to conduct training" is included, the overall majority of respondents are engaged in targeted e-mail training.

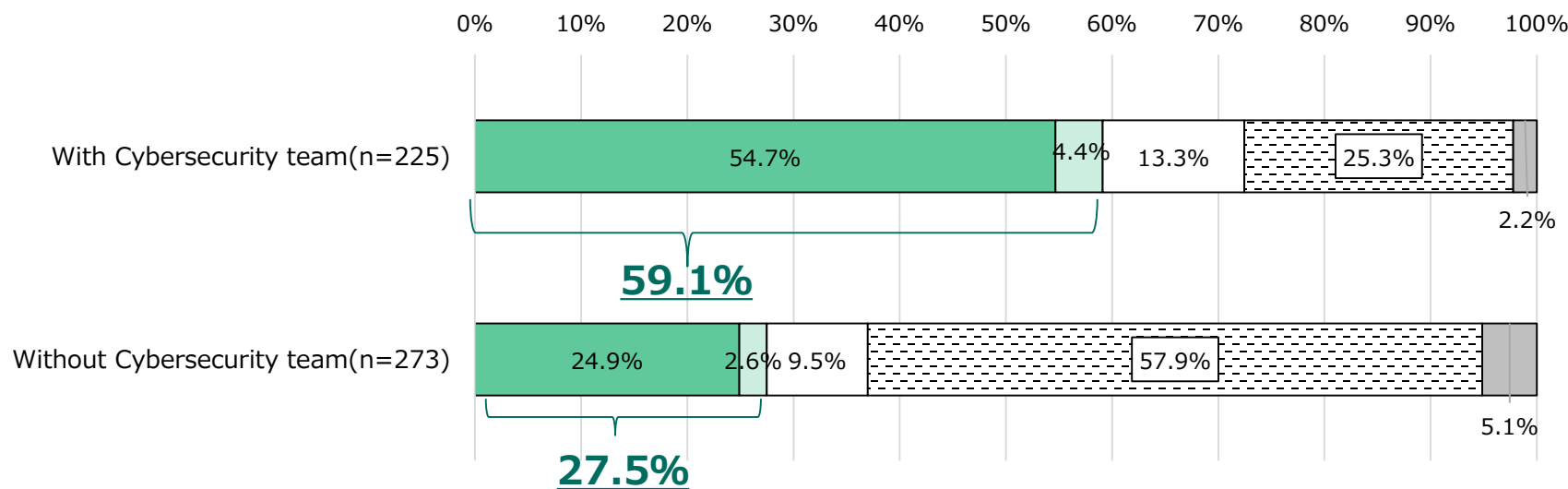
Compared to the aforementioned security incident training on a wide range of topics, the percentage of companies conducting training is high, suggesting that targeted email attacks are becoming a **more familiar threat** to companies.



## Training for incoming suspicious emails (targeted email training) (2/2)

A large number (**59.1%**) of companies with an organizational structure responded that they "conduct training (total number of practice with non-IT dept. and Practice only IT dept.). On the other hand, less than 30% (**27.5%**) of companies without an organizational structure responded.

Establishing an organizational structure as well as security incident training is the first step to strengthen the security system afterwards.



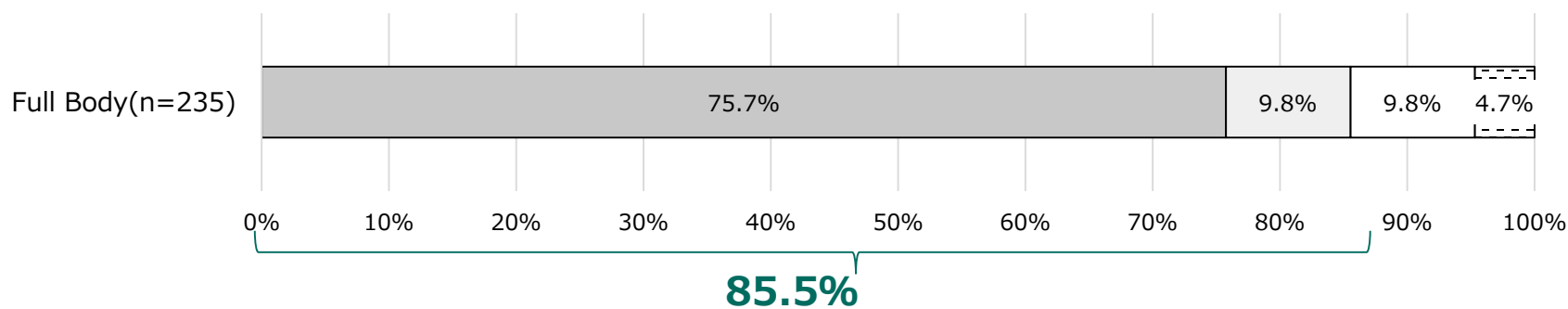
- Practice with non-IT dept.
- Practice only IT Dept.
- Plan to have practice
- ▨ No practice and No Plan
- Other

## Whether or not to review the results of training for suspicious incoming e-mails (targeted e-mail training) (1/2)

(If you answered "1. Training is conducted (non-IT departments also participate)" or "Training is conducted (IT departments only)" in the previous question)

The number of companies that are currently reviewing the results of the training and the content of the training accounted for **75.7%** of the total, and if the companies that are planning to review the content of the training (9.8%) are included, **more than 80%** of the companies are reviewing/planning to review the content of the training.

**In targeted email attacks, it is difficult to reduce the open rate to zero, so it is important to provide education and training so that when an email is opened, it can be quickly and appropriately reported and dealt with.**



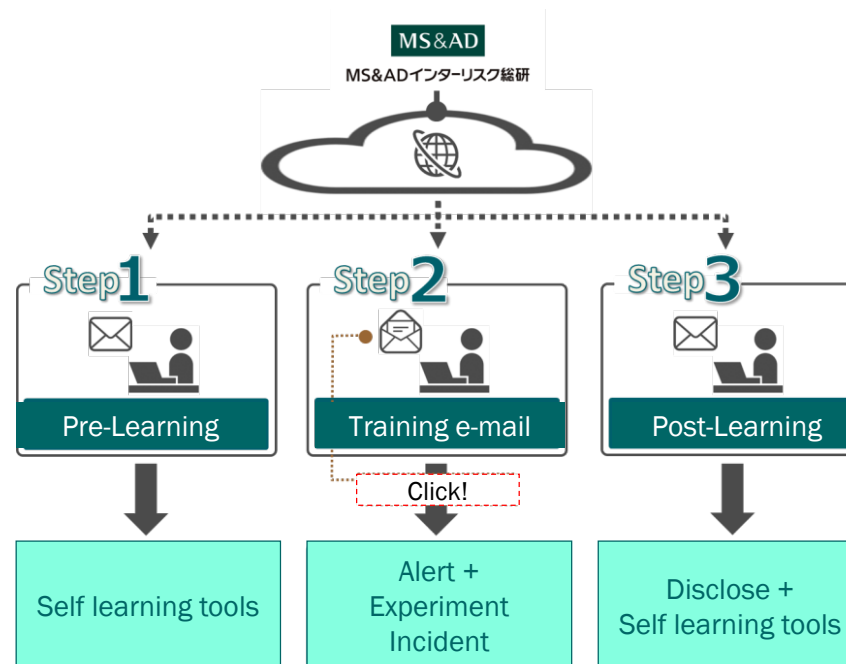
- reviewing the results of the training and the content of the training accounted
- planning to review the content of the training
- Not reviewing
- Other



## Whether or not to review the results of training on suspicious incoming e-mails (targeted e-mail training) (2/2)

(If you answered "1. Training is conducted (non-IT departments also participate)" or "Training is conducted (IT departments only)" in the previous question)

**The** targeted e-mail training service we provide comes in two patterns: a full package plan that includes three learning opportunities: "pre-learning," "training e-mail," and "post-learning," and a plan that includes only "training e-mail. The full package plan accounts for more than 70% of the services offered, indicating **that there is a need for training that includes "actions to be taken when a targeted e-mail is opened".**

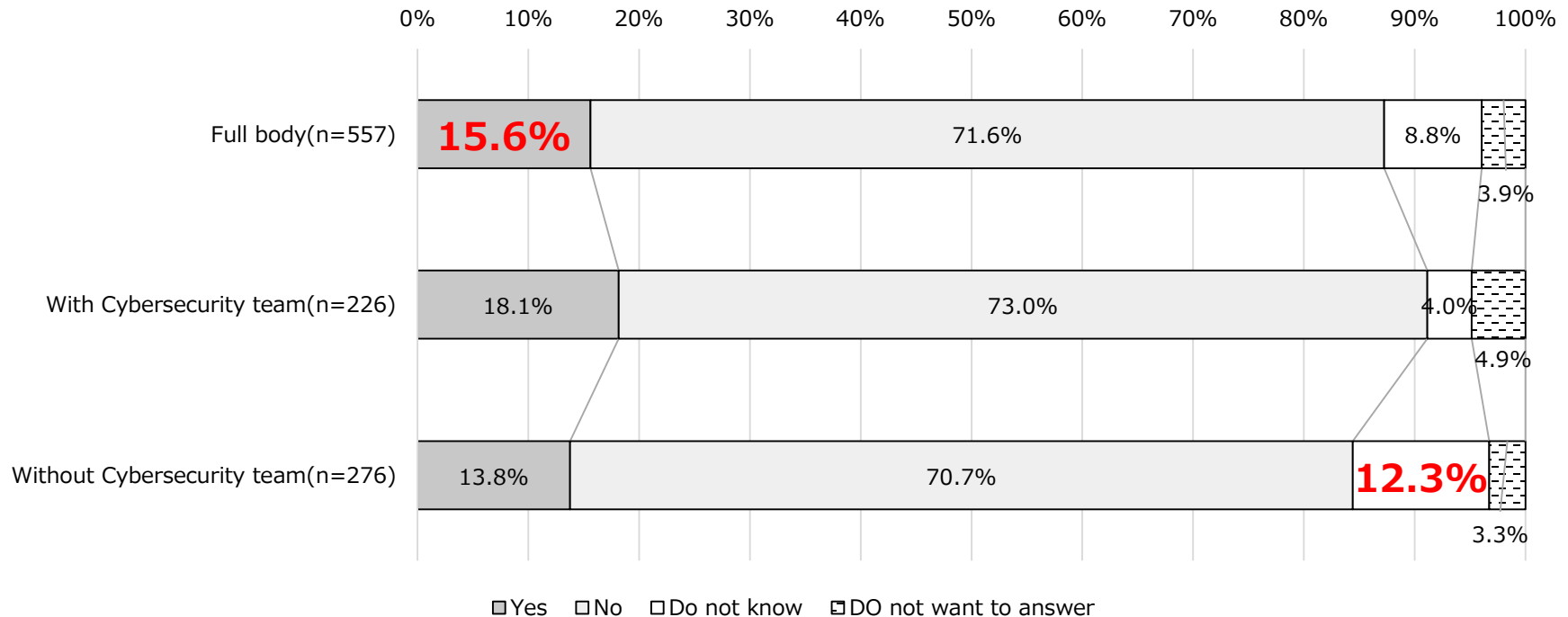


## Occurrence of cyber security incidents

## Past cyber security incidents (1/2)

When asked if there had been any cyber security related incidents in the past, **15.6%** of the companies answered "yes".

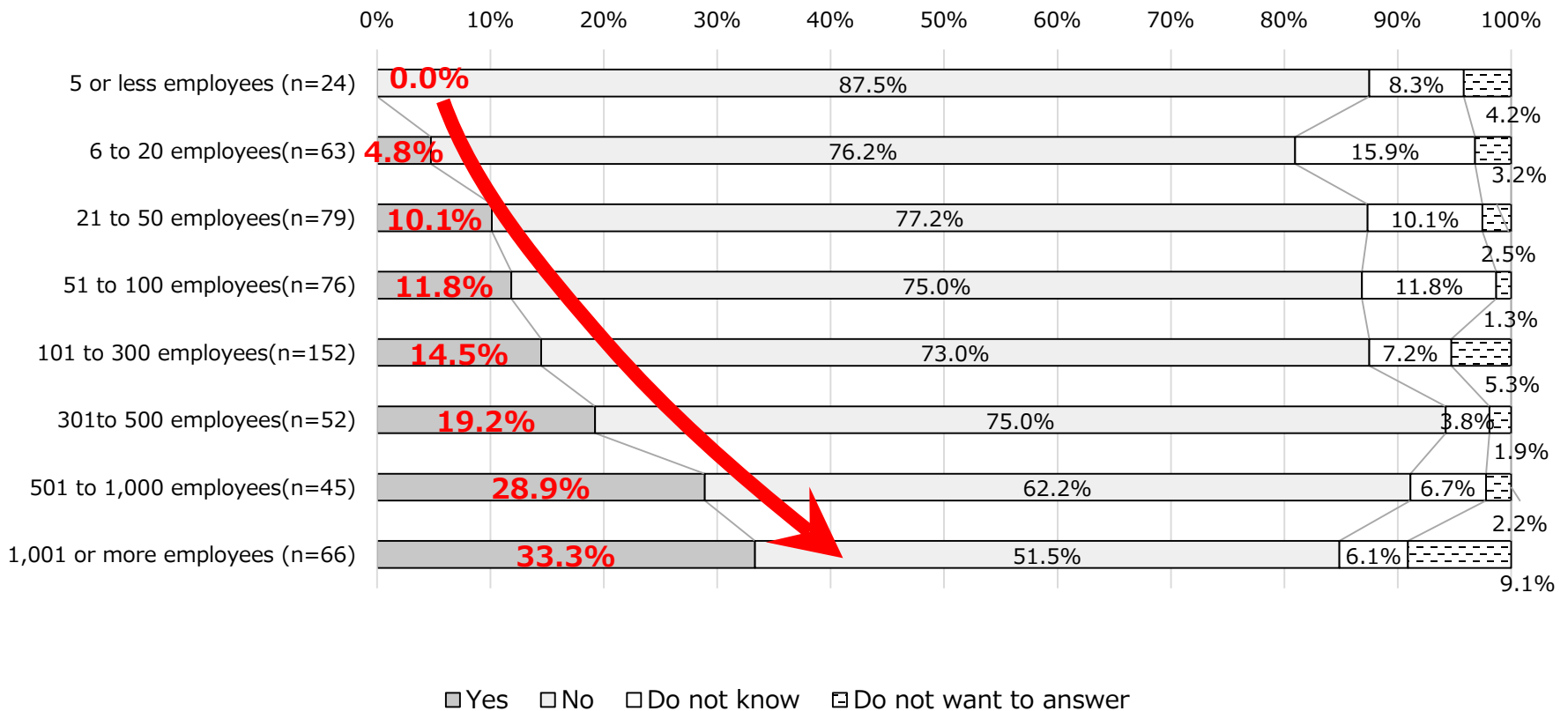
Looking at the results by organizational structure, a high percentage (**12.3%**) of companies with no structure responded that they "do not know or do not understand," suggesting that even if there were accidents, they may not have been detected in the first place.



## Cyber security incidents in the past

When compared by the number of employees, the percentage of companies that responded that an accident had occurred was higher for companies with more employees.

In addition to indiscriminate attacks, large companies are more likely to meet cyber attacks as the ultimate target of targeted attacks and supply chain attacks, I would guess.

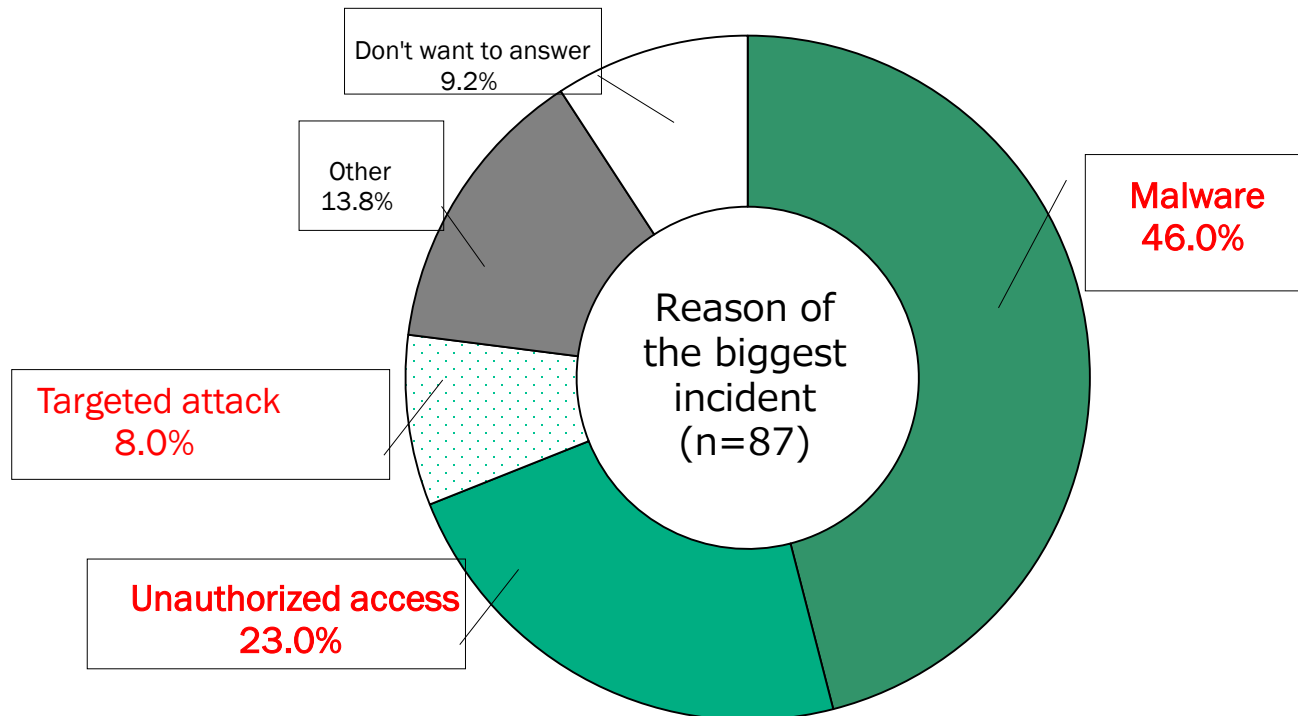


## Details of the most damaging cyber security incidents

(If you answered "have had a cyber security incident")

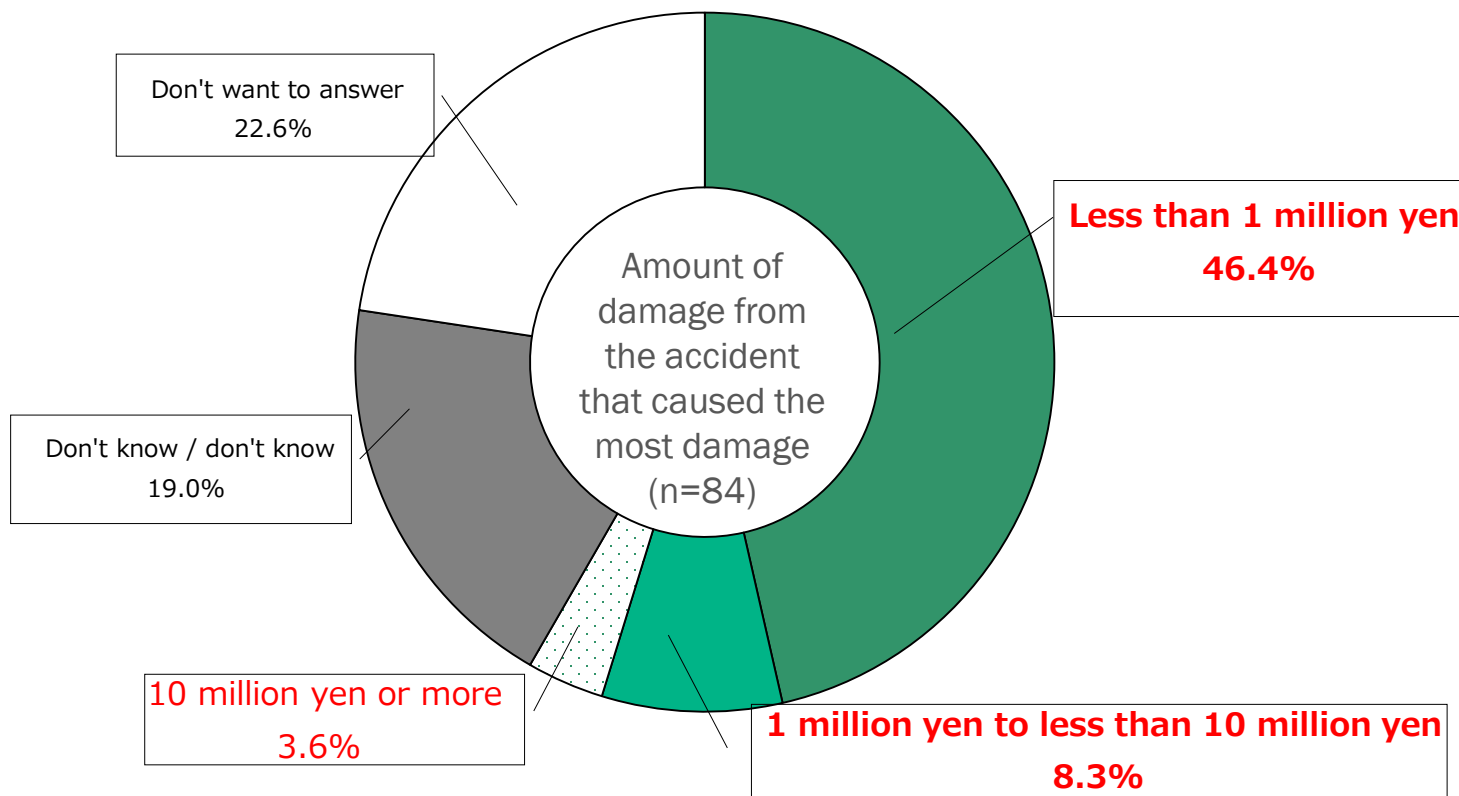
When the contents of the most damaging cyber security incidents that occurred in the past were checked, **malware (46.0%)**, **unauthorized access (23.0%)**, and **targeted attacks (8.0%)** were ranked first, second, and third, respectively.

The "Other" category includes "Insider", "Rewriting of HP/web pages", "Hijacking of e-mail accounts", and "DDoS attacks" and others.



## Amount of damage from the most damaging cyber security incidents (If you answered "have had a cyber security incident")

Among the cyber security incidents that occurred in the past, when we checked the amount of damage of the most damaging incident, the first place was less than 1 million yen (46.4%), the second place was between 1 million yen and 10 million yen (8.3%), and the third place: 10 million yen or more (3.6%).

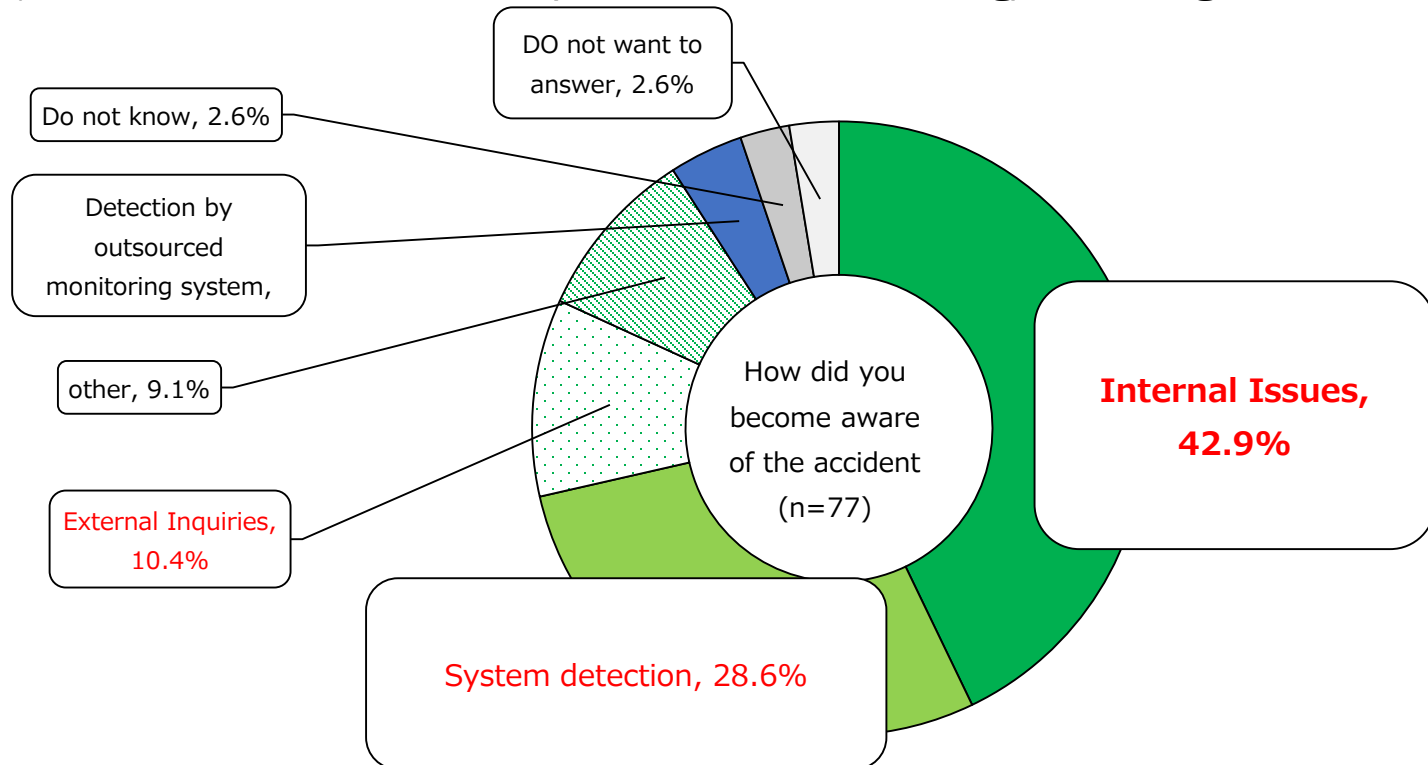


## How did you become aware of the accident?

(In the case of respondents who answered "the most damaging cyber security incident")

When asked how they recognized cyber security related incidents, the largest number of companies (**42.9%**) answered "report from employees themselves". This was followed by "detection by the system (including internal monitoring system (**28.6%**)" and "notification or inquiry from outside the company (**10.4%**)".

The "Others" category included responses such as "Deterioration in risk score (external evaluation)" and "Deterioration in response time for sending/receiving e-mails."



# Cyber insurance



## Cyber Insurance / data breach Insurance (1/2)

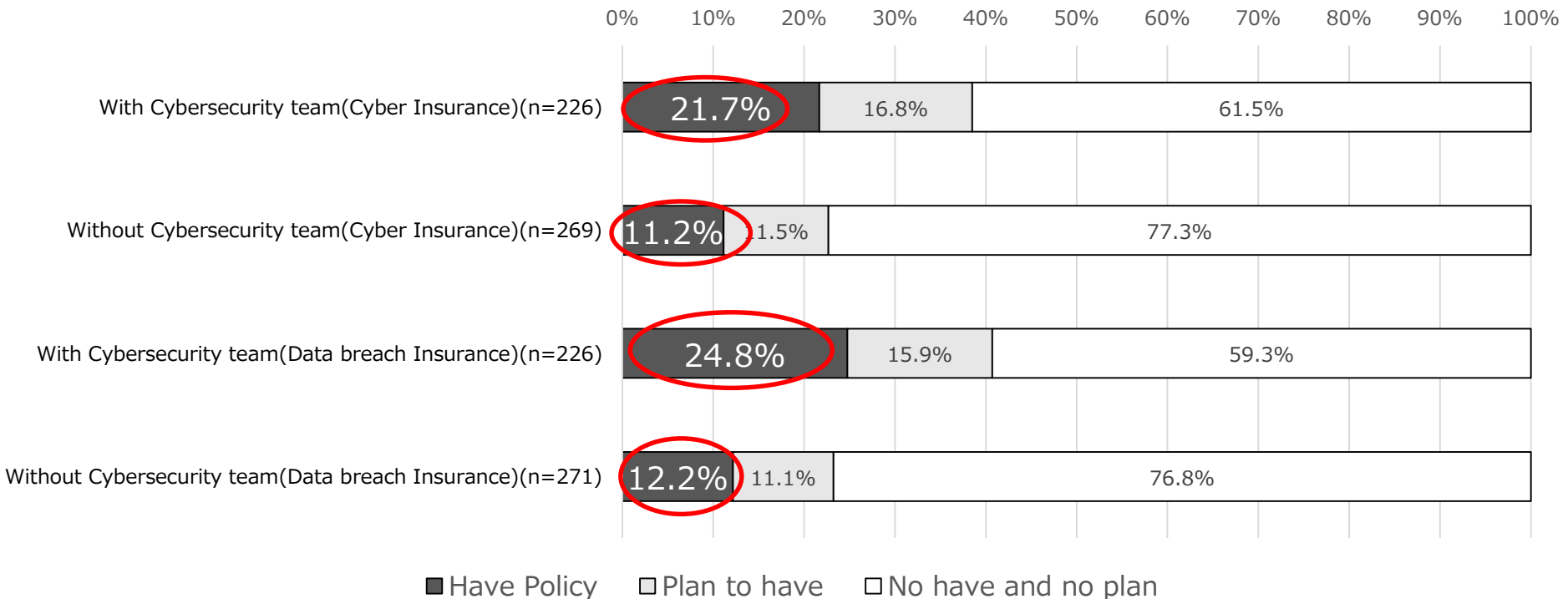
More than 80% of the companies “No have” cyber insurance or data breach insurance policy, respectively. **16.8%** of the companies have cyber insurance policy and **18.8%** **have** data breach insurance policy, which is low for the overall participation status.



## Cyber Insurance/Data breach Insurance Participation Status (2/2)

In terms of organizational structure, there is a difference in insurance coverage between companies with and without a structure. For example, the rate of **cyber insurance** coverage was **21.7%** for those with cybersecurity team, double the rate for those without team(**11.2%**).

The rate of **data breach insurance** was **24.8%** for those with cybersecurity team, while it was **12.2%** for those without team, also doubling.



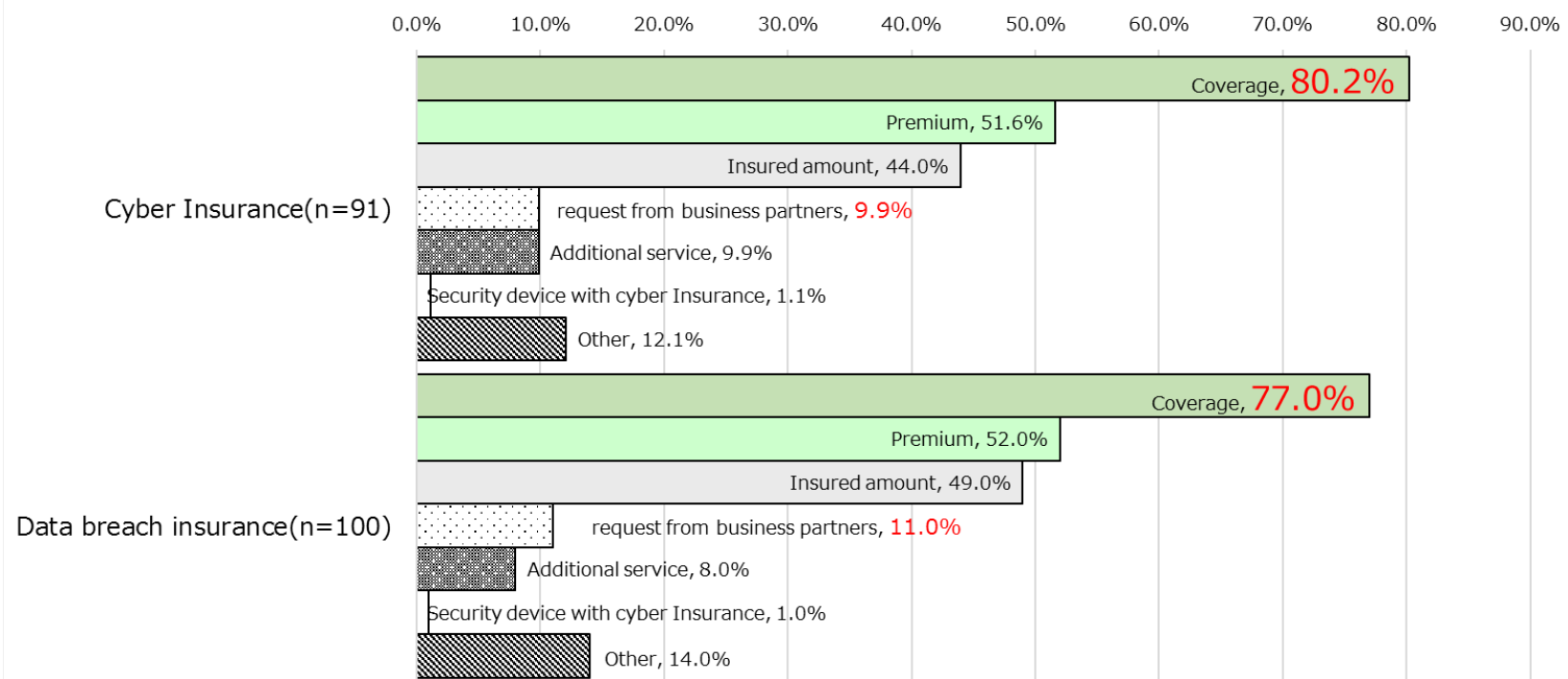
## Deciding factor for purchasing insurance\* Multiple choices

(If you answered "Yes" to the previous question)

For both cyber insurance and data breach insurance, the most common reason for purchasing insurance was that the **coverage was suitable for the company (80.2% for cyber insurance and 77.0% for data breach insurance).**

Only **about 10%** of the companies in both cyber insurance and data breach insurance cited **"requests from business partners"** as the reason.

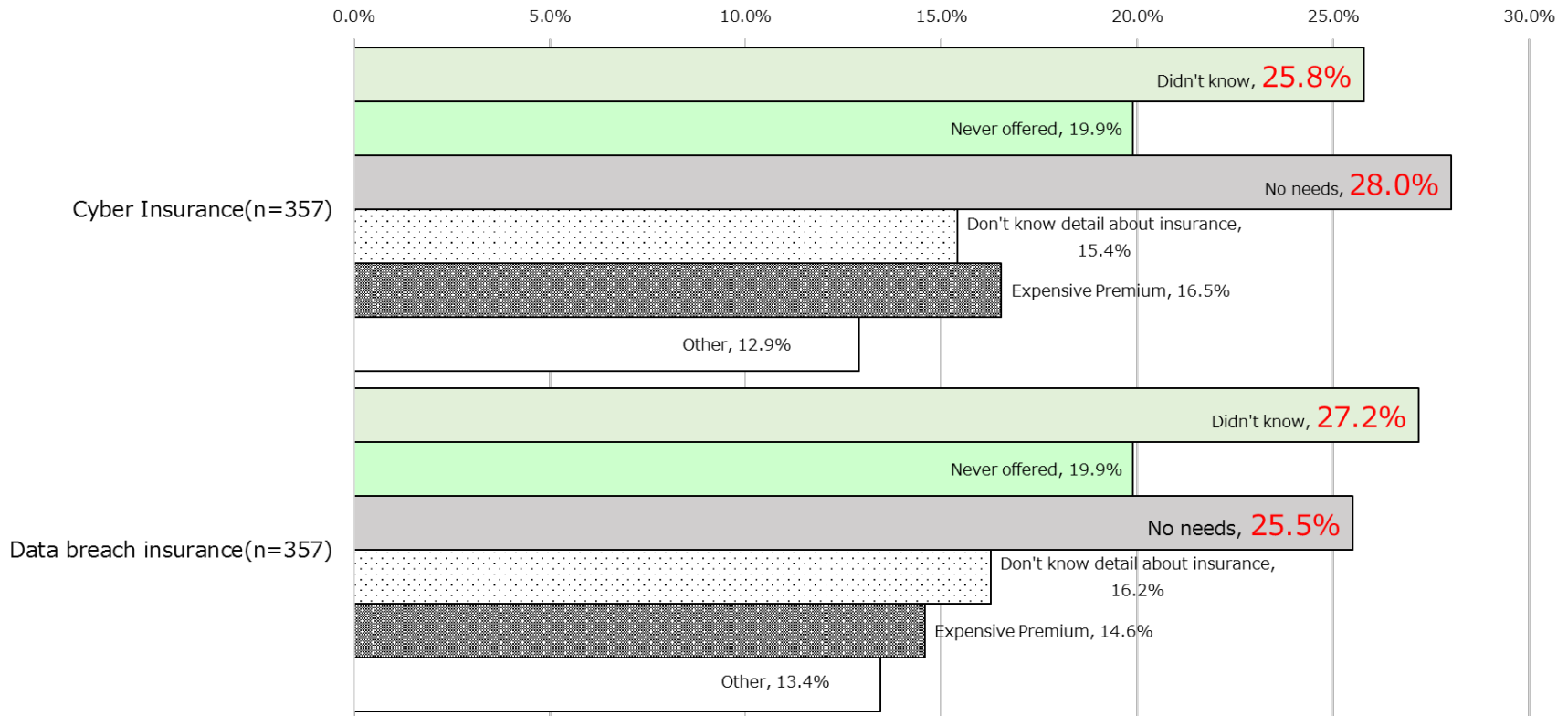
In the "Other" category, there were responses such as "Lump-sum contract by parent company/group company" and "Request from parent company/head office."



## Reasons for not having insurance\* multiple choice (1/2)

(If you answered "Considering" or "Have not joined" in the previous question)

As reasons for not purchasing insurance, a certain number of companies answered that they **did not know the insurance existed** (cyber insurance: 25.8%, data breach insurance: 27.2%) or that they **don't need the insurance** (cyber insurance: 28.0%, data breach insurance: 25.5%).

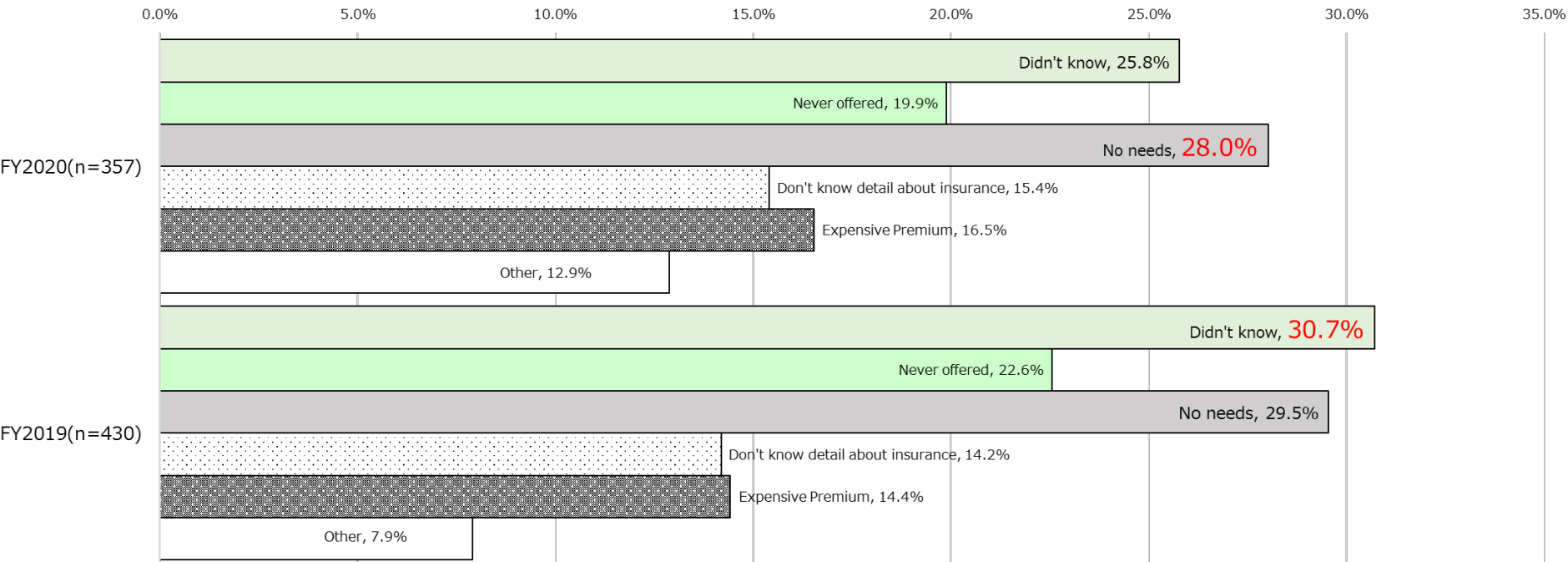


## Reasons for not having insurance\* multiple choice (2/2)

(If you answered "Considering" or "Have not joined" in the previous question)

The reasons for not purchasing cyber insurance were compared with the previous year's survey. **The most common answer last year was "I didn't know there was cyber insurance (30.7%)".**

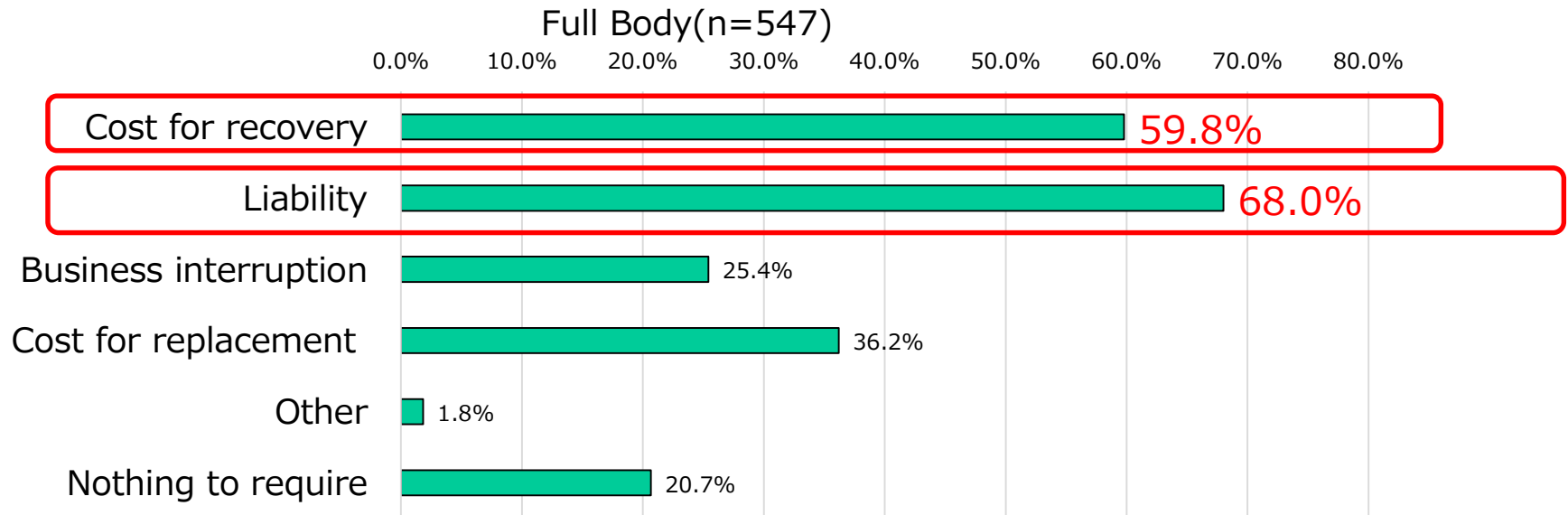
**However, the most common response this year was "I don't need the insurance (28.0%)."** While the awareness of cyber insurance is increasing, the number of companies that do not feel the need to purchase it is also increasing.



## What you want to be covered by cyber insurance\* Multiple choices

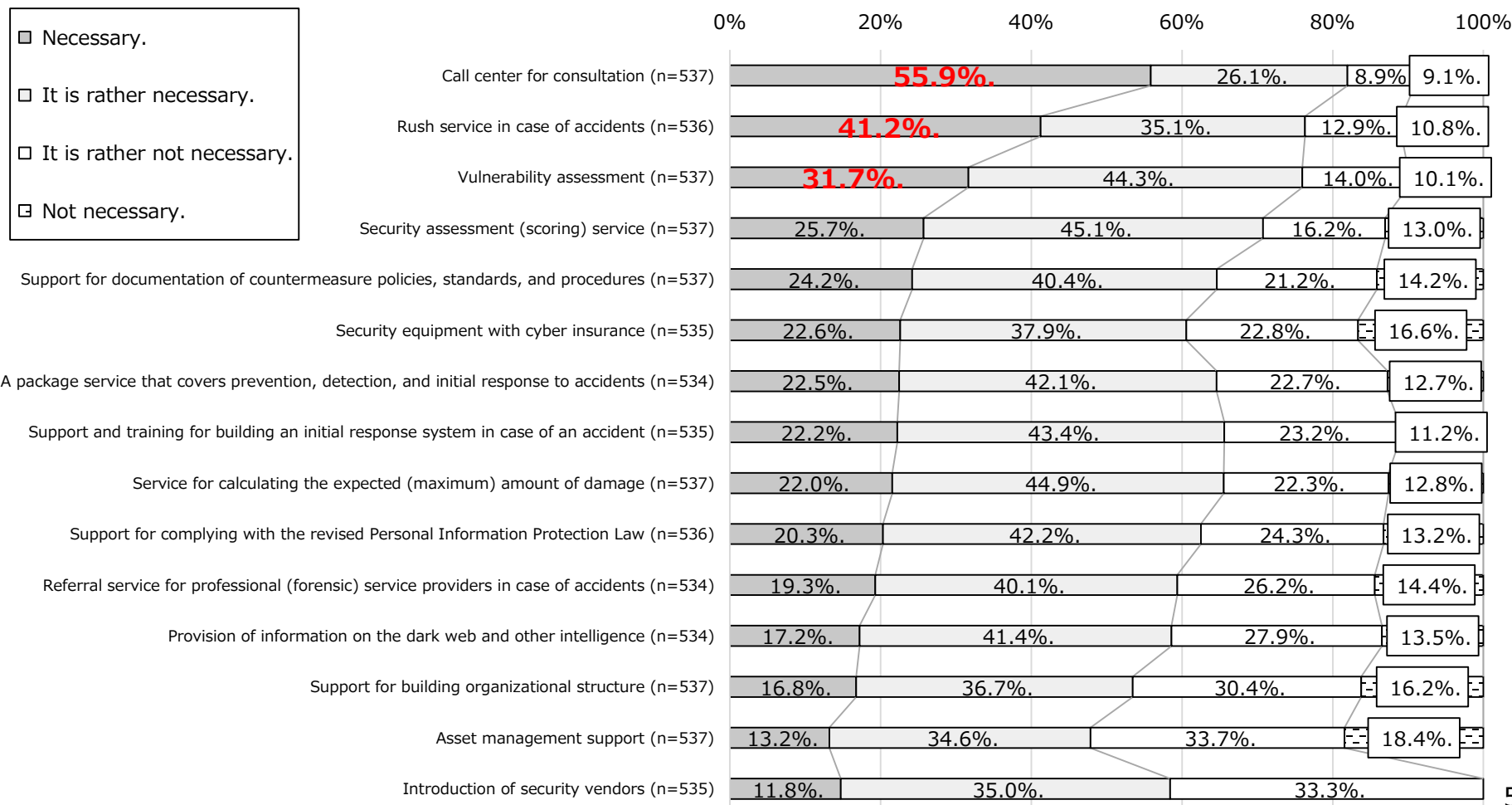
The most common loss expected to be compensated by insurance was "compensation for damages in the event of an data breach" (68.0%), followed by "response and restoration costs" (59.8%).

Among the "Others," there were responses such as "expenses for lawyers and advisors to deal with the media in the event of an incident."



## Expect as a supplementary service for cyber insurance








As for the expected services, the highest expectation was for the **consultation call center (55.9%)**, the **rush service in case of accidents (41.2%)**, and **vulnerability assessment (31.7%)**, in that order.



## Expect as a supplementary service for cyber insurance

When we ranked the expected services for both overall and companies that do not have cyber insurance, we found a similar trend, but for companies that do not have insurance, "a package service that includes protection, detection, and initial response in the event of an accident (23.4%)" was the top choice.

**The uninsured were found to have a need for added value that would lead to protection, detection, and initial response, not just after-the-fact measures.**

whole		Companies that do not have cyber insurance		
Rank	Expectations for ancillary services	Rank	Expectations for ancillary services	2020
1	Consultation call center (55.9%)	1	Consultation call center (57.5%)	
2	Rush service in case of accidents (41.2%)	2	Rush service in case of accident (42.6%)	
3	Vulnerability assessment (31.7%)	3	Vulnerability assessment (33.2%)	
4	Security diagnosis (scoring) services (25.7%)	4	Security diagnosis (scoring) services (25.1%)	
5	Support for preparing documents on countermeasure policies, standards, procedures, etc. (24.2%)	5	A package service that combines prevention, detection, and initial response to an accident <b>(23.4%)</b>	
6	Security equipment with cyber insurance (22.6%)	6	Security equipment with cyber insurance (23.2%)	
7	A package service that combines prevention, detection, and initial response to an accident (22.5%)	7	Support for preparing documents on countermeasure policies, standards, procedures, etc. (22.9%)	

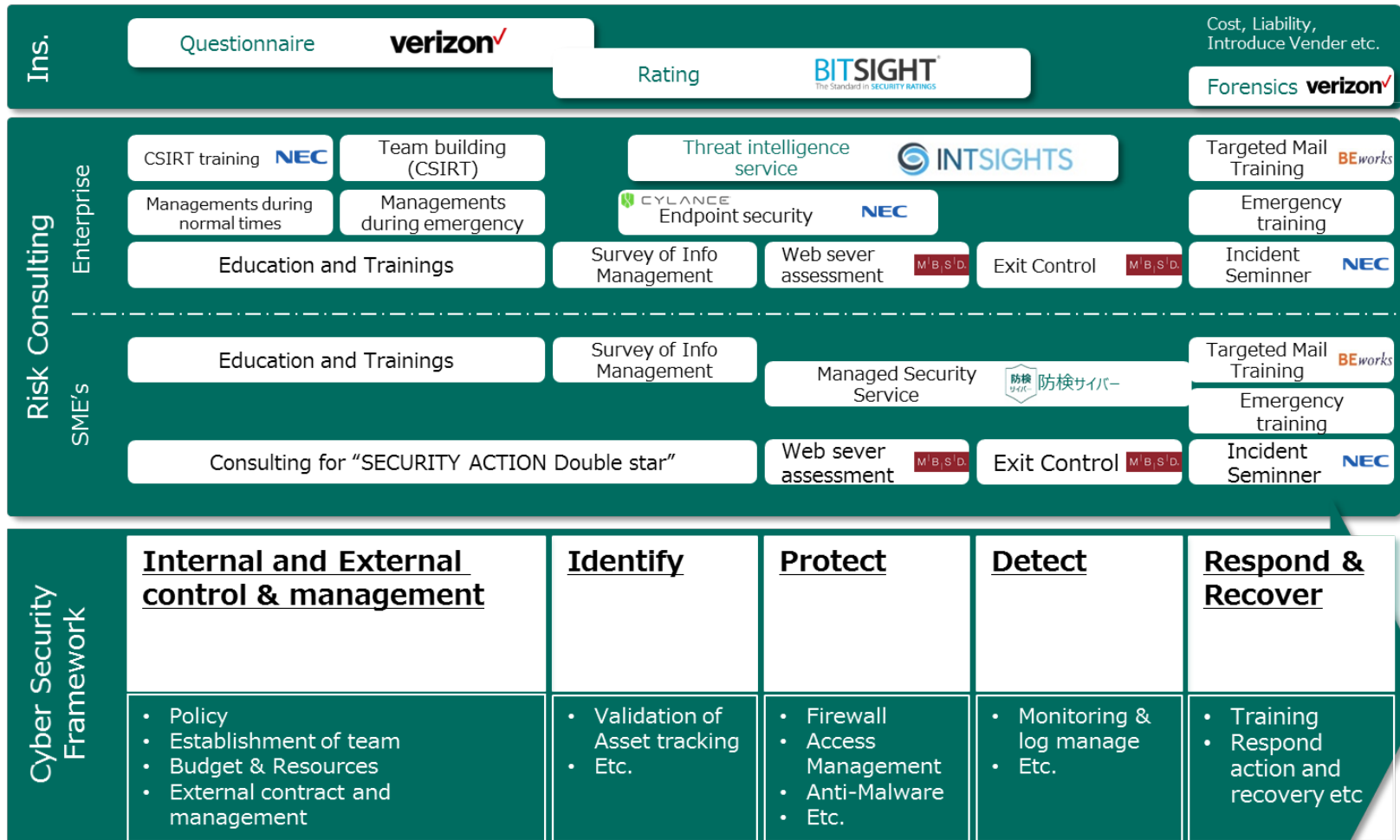


## What to expect as a supplementary service when you purchase cyber insurance (2/2)

whole		Companies that do not have cyber insurance		
Rank	Expectations for ancillary services	Rank	Expectations for ancillary services	2020
8	Support and training for building an initial response system in the event of an accident (22.2%)	8	Support and training for building an initial response system in the event of an accident (20.8%)	➔
9	Calculation service of expected (maximum) loss (22.0%)	9	Calculation service of expected (maximum) loss (20.2%)	➔
10	Support for compliance with the revised Personal Information Protection Law (20.3%)	10	Support for compliance with the revised Personal Information Protection Law (19.9%)	➔
11	Referral service for professional (forensic) service providers in case of accidents (19.3%)	11	Referral service for professional (forensic) service providers in case of accidents (17.0%)	➔
12	Providing intelligence information on the dark web, etc. (17.2%)	12	Providing intelligence information on the dark web, etc. (16.8%)	➔
13	Support for building organizational structure (16.8%)	13	Support for building organizational structure (16.3%)	➔
14	Asset management support (13.2%)	14	Asset management support (12.3%)	➔
15	Referrals from security vendors (11.8%)	15	Referrals from security vendors (9.6%)	➔

# Cyber Security and MS&AD Platform

The MS&AD Group has compiled solutions corresponding to the Framework for Cyber Security as the "MS&AD Cyber Security Platform. Please use this platform when you take cyber security measures, such as using a specialized service provider if you are unable to take measures by yourself, or purchasing insurance as a countermeasure for remaining risks.



**MS&AD**

# **MS&AD Insurance Group**

**MS&AD InterRisk Research Institute, Inc.**  
Cyber Risk Sec., New Business Development Dept.

Wateras Annex, 2-105 Awaji-cho, Kanda, Chiyoda-ku, Tokyo 101-0063, Japan

Tel : +813-5296-8961 / Fax : +813-5296-8940

<https://www.irric.co.jp/>