Research of SMB's Cybersecurity measures in Japan 2019

MS&AD InterRisk Research & Consulting

Introduction

Introductions

<Introductions>

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.

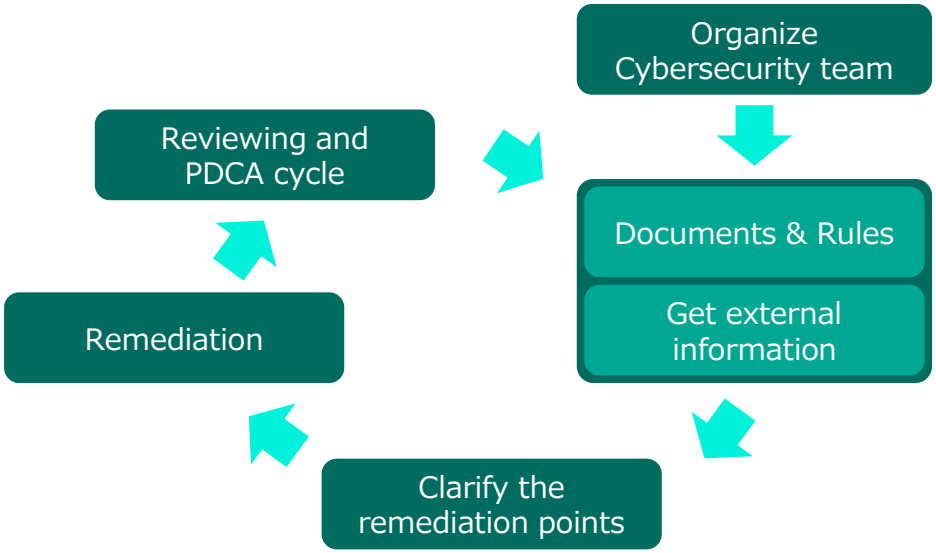
We hope this survey will be helpful to companies for further efforts.

Introductions

<Insights>

① Companies that have an organized Cybersecurity Team (structure) have advantageous results in Cybersecurity measures as well as rates of having cyber insurance. One of the reasons for measures to be taken by developing the organizational structure is that making 'what should be implemented' clearer by external information which is provided from organizations outside the company (ex. Nippon CSIRT Association, JNSA, IPA, etc.).

② In addition to the organizational structure improvement, the policy ⇒ standard ⇒ procedure, that the correspondence with documents and rules also developed into more practical one is also a point as a matter of actual security measures.



③ As the usage of the cloud service by SMB expands in the future, "Develop a model of a recommended system architecture includes cloud services which are trusted by SMBs for utilization" can be mentioned as a countermeasure.

④ Companies without Cybersecurity Team need to contract a services that can treat the possibility of cyber accidents (incidents) when the total damage is still small.

⑤ About cyber insurance, companies are not understanding its existence and contents (compensation scope, targeted accident, etc.).

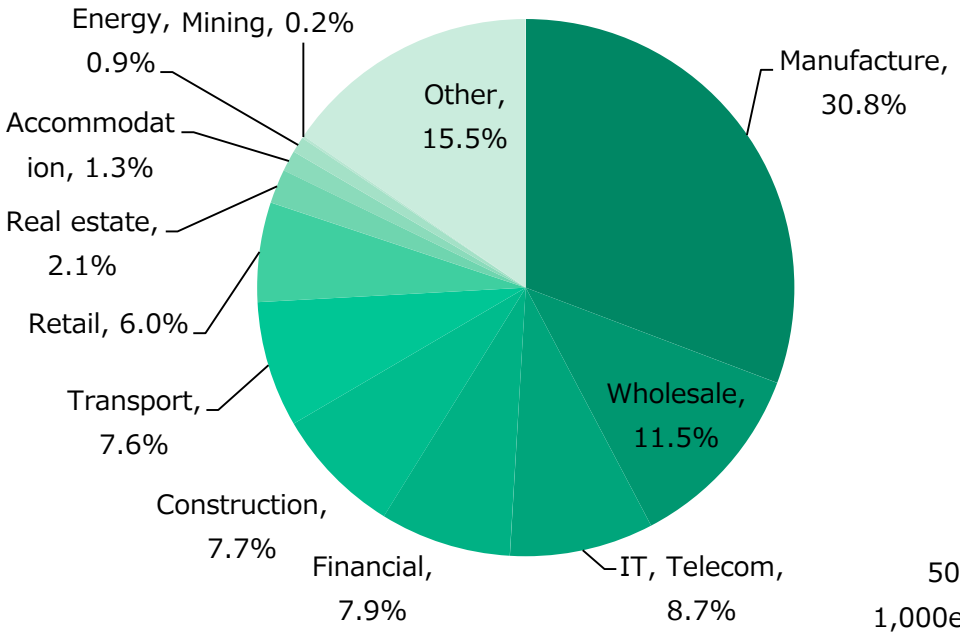
Overview of the Research

Advancing with you
MS&AD
INSURANCE GROUP

Overview of the Research

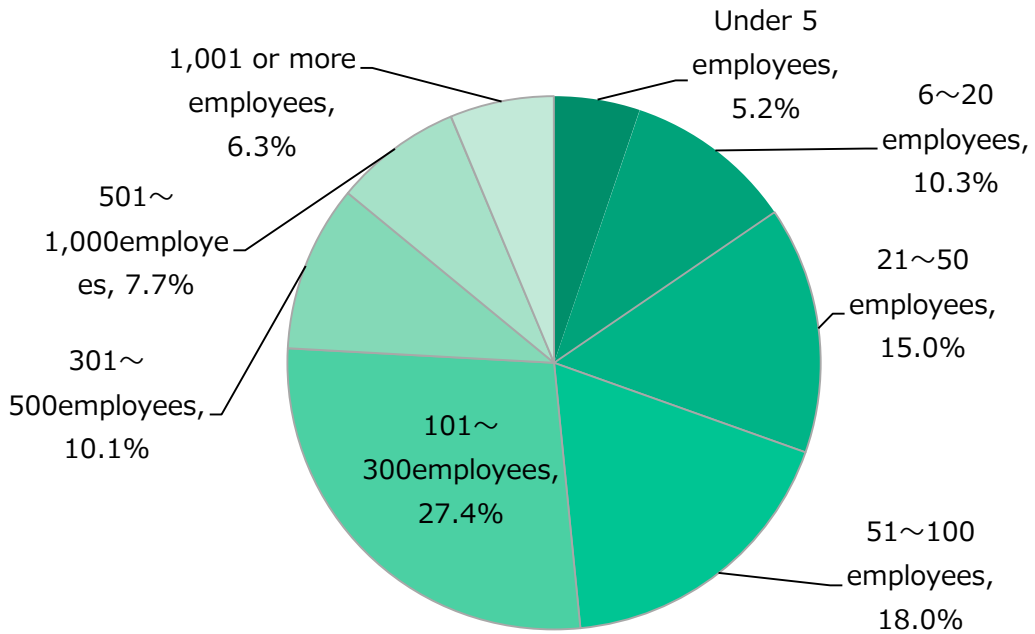
Survey method	Mailing questionnaire (combined with Web response)
Targeted companies	10,000 companies in Japan Extracted from Toyo Keizai Inc.'s "40,000 company data in Japan ((1) Basic data)" Companies that randomly extracted in industry by industry
Number of valid responses	634 (total collected number: 644) Recovery rate 6.3%
Survey period	November 13 - November 30, 2019

Industry and size of the companies



(n=634)

(n=634)

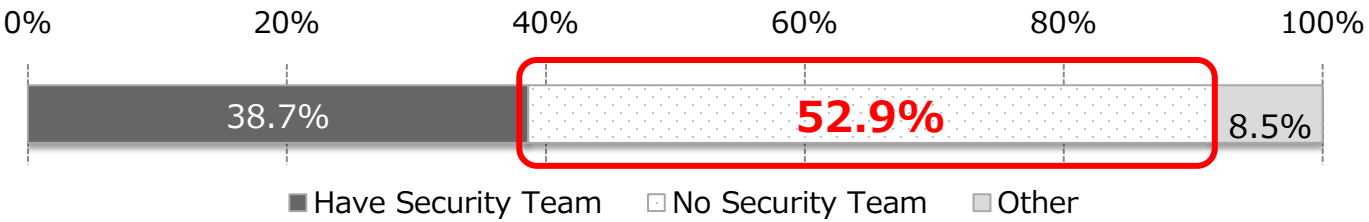


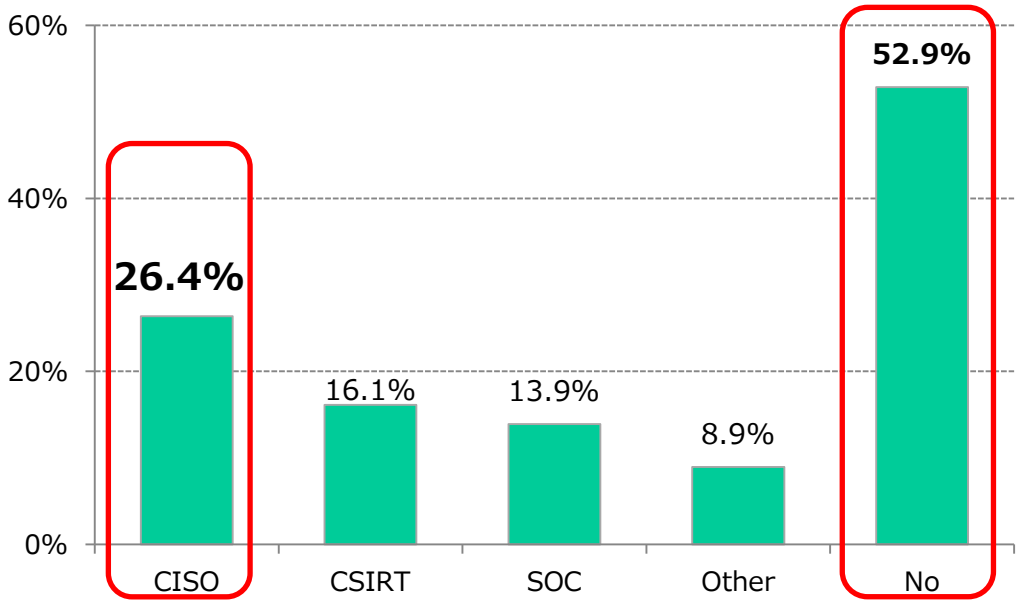
Internal Organization Management

Cybersecurity Team *Multiple selection

The majority of responding companies have not established a cybersecurity team. But **"CISO"** is most popular in the companies that replied "Yes".

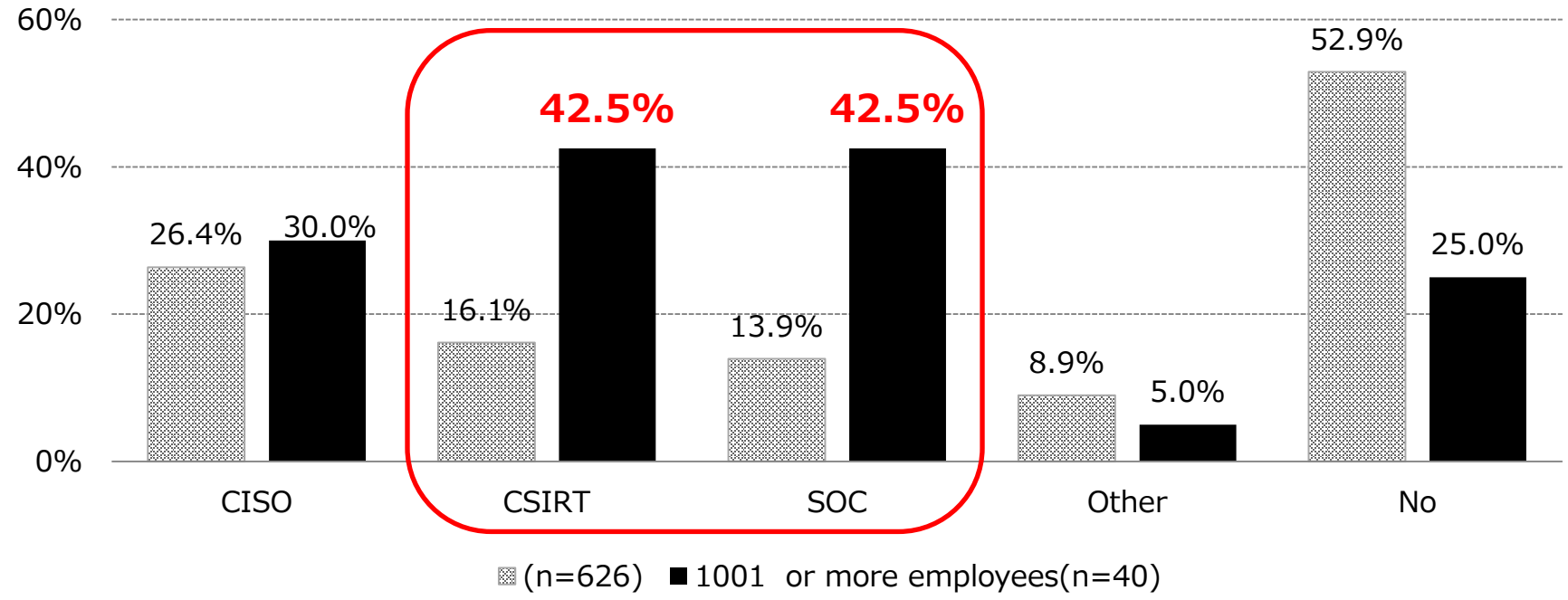
ALL(n=626)





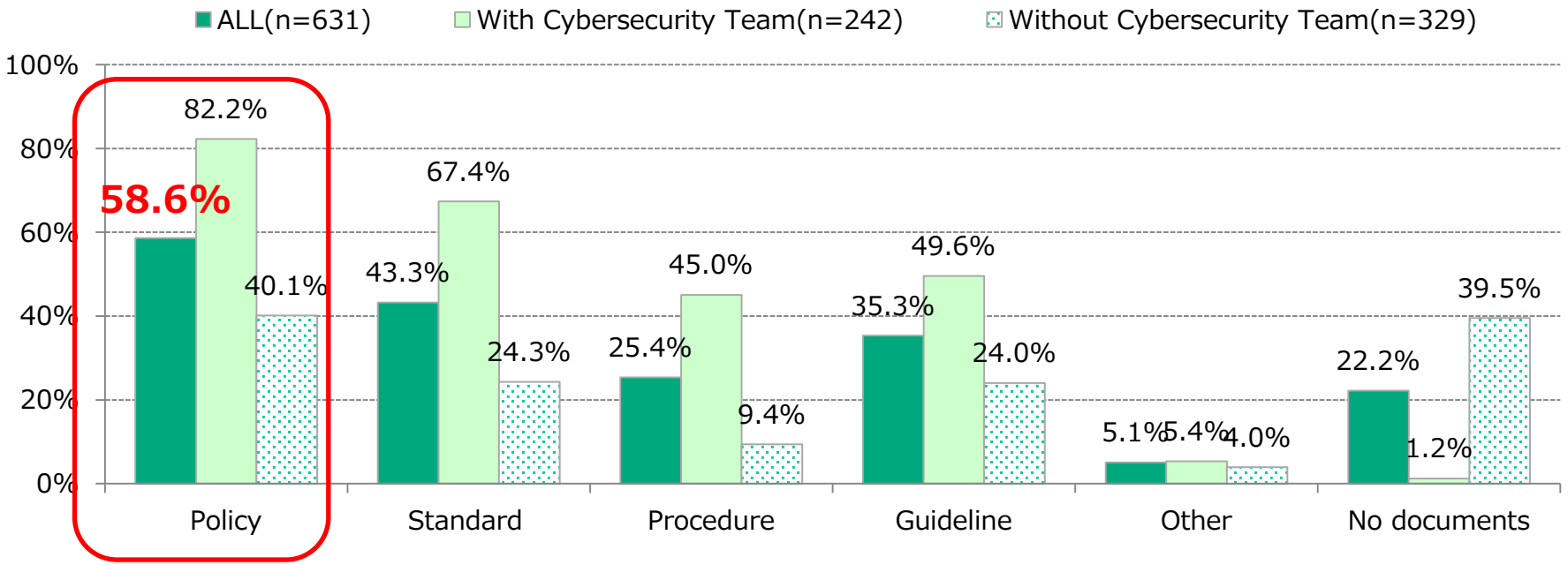
Cybersecurity team established *Multiple selection

Looking further by the number of employees, **42.5% of companies with more than 1,001 employees are establishing "CSIRT“ and/or "SOC“**, and the organization size is considered to be related to the establishment of Cybersecurity team.
The percentage of enterprises that have “SOC" has increased significantly from 2018.（2018:27.7%→2019:42.5%）。



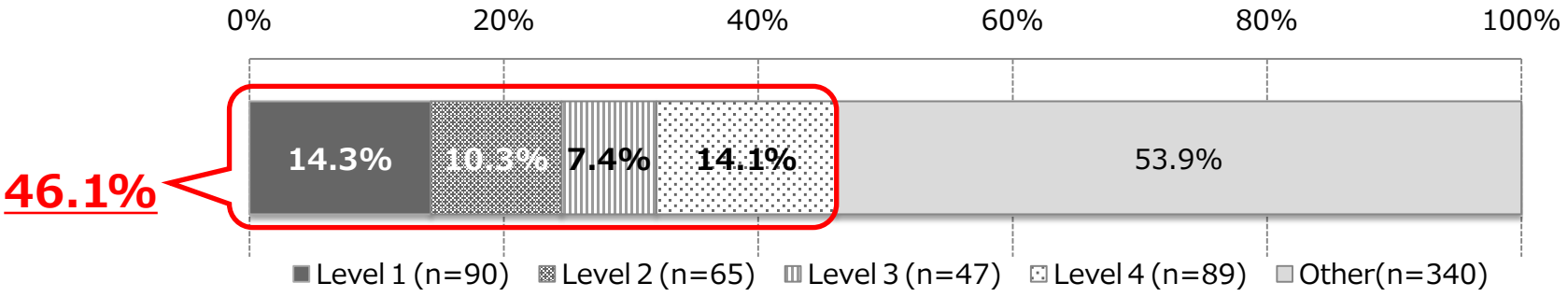
Documents for cybersecurity *Multiple selection

"Policies" (**58.6%**) are most frequently maintained as cybersecurity documents and regulations.
In the "Other", there were answers such as 'It complies with the group company/parent company', 'It is incorporated in the company regulations such as rules of employment' and etc..
In the "No documents", there were answers such as 'There is no department in charge.', 'Cost' and etc..



Documents for cybersecurity *Multiple selection

Assuming that the status of development of security documents is to be improved with policy ⇒ standard ⇒ procedure ⇒ guidelines and classified into 5 categories according to level as below, nearly half of companies organize documents in order.

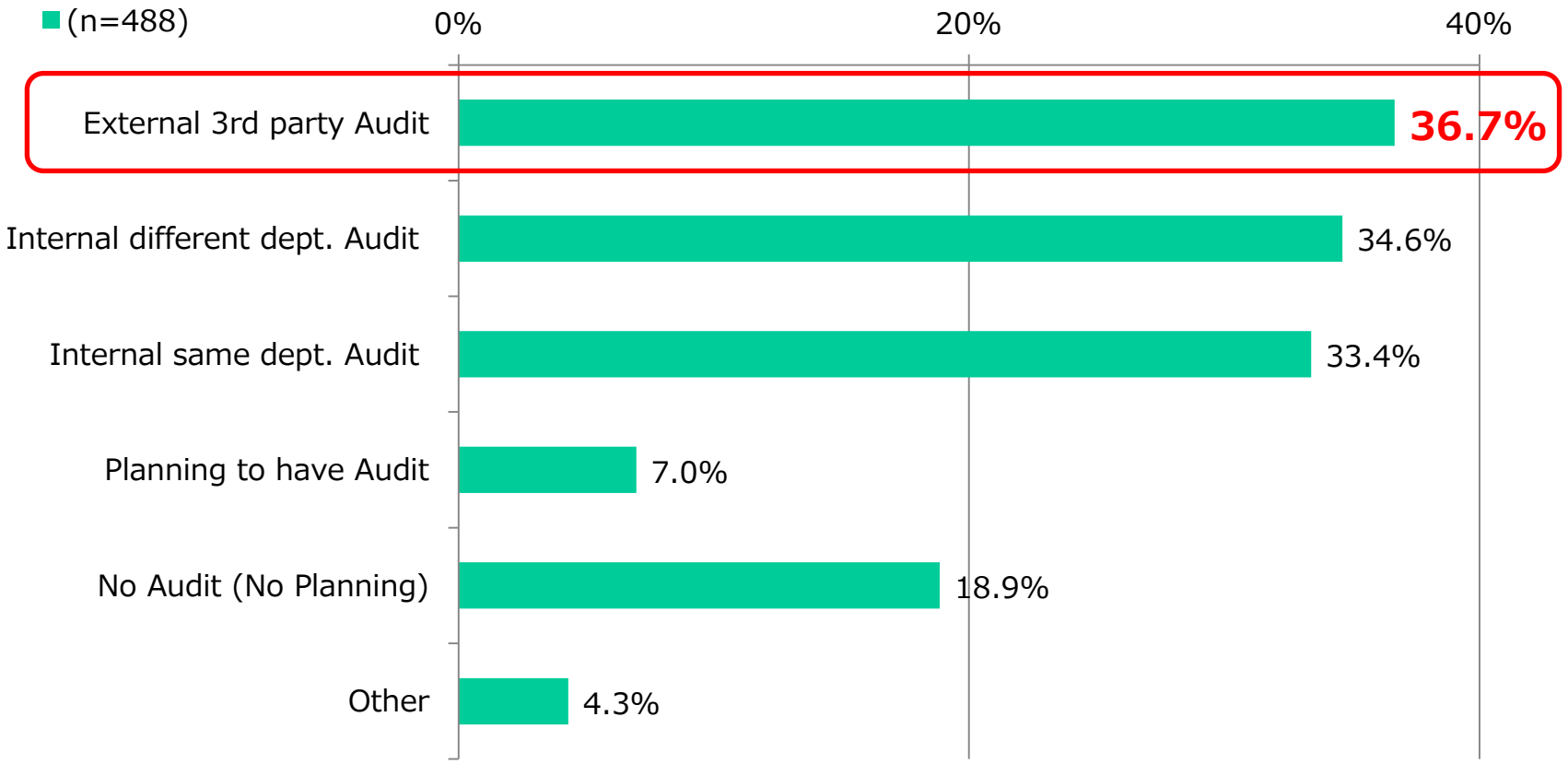


	Policy	Standard	Procedure	Guideline
Level 1	○	—	—	—
Level 2	○	○	—	—
Level 3	○	○	○	—
Level 4	○	○	○	○
Other	–			

Audit of the documents *Multiple selection

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

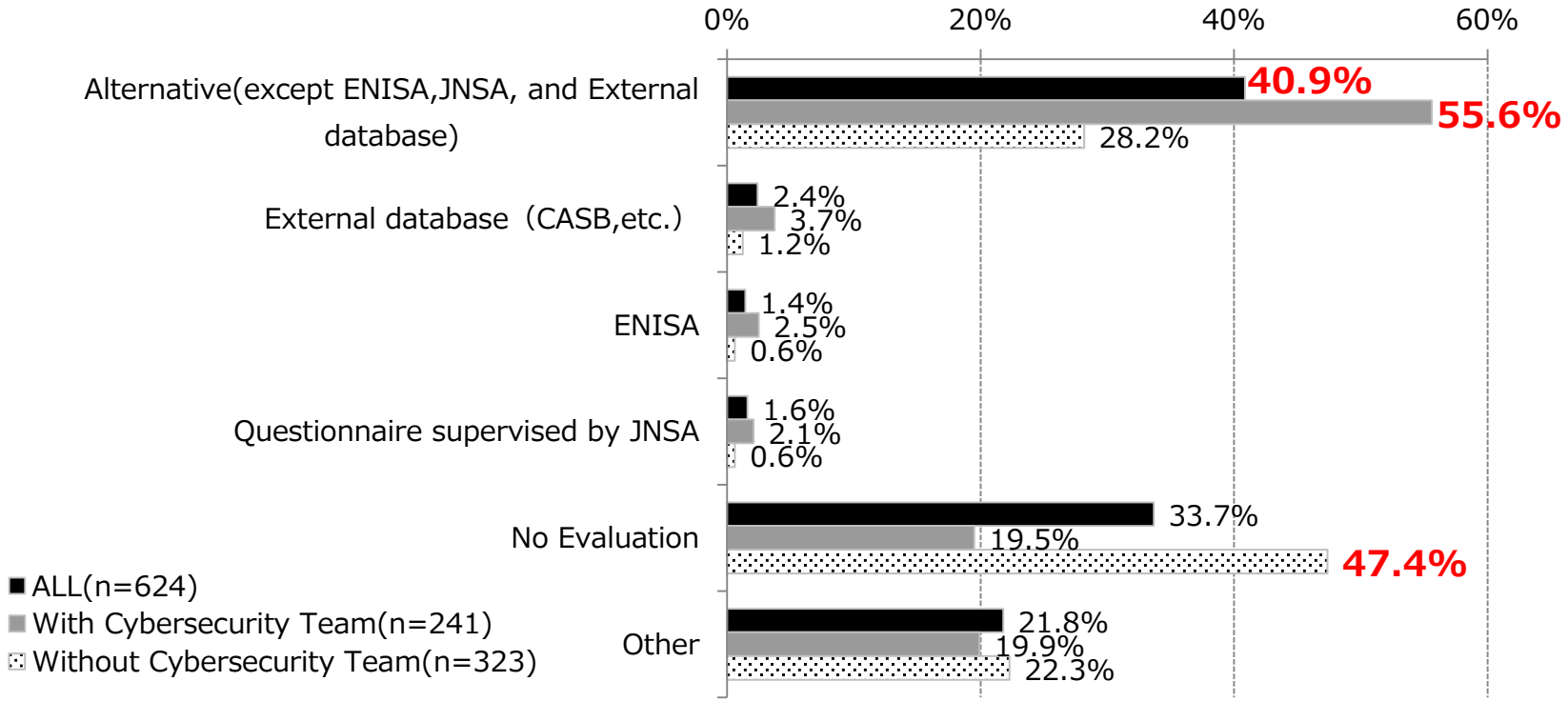
36.7% of the companies chose “External 3rd party Audit”.



3rd Party (Subcontractor) Management

Security Evaluation at Cloud Service Providers Selection

40.9% of the companies chose “Alternative”.
55.6% for companies with Cybersecurity team chose “Alternative”.
On the other hand, **47.4%** for companies without Cybersecurity team choose ”No Evaluation” at the moment of Cloud Service Purchase.
In the “Other”, there were answers such as “Guide book by IPA” and etc..



Advancing with you
MS&AD
INSURANCE GROUP

Security Evaluation at Cloud Service Providers Selection

67.5% of companies with more than 1,001 employees choose “Alternative”, while **17.5%** of those companies choose ”No Evaluation”. In addition, companies with more than 51 employees execute a security assessment and on the other hand, companies with under 50 employees don’t evaluate.

In the future, we are required to develop a model of the recommended system configuration including cloud services that can be used safely by enterprises.

Identify

Handling status of information assets

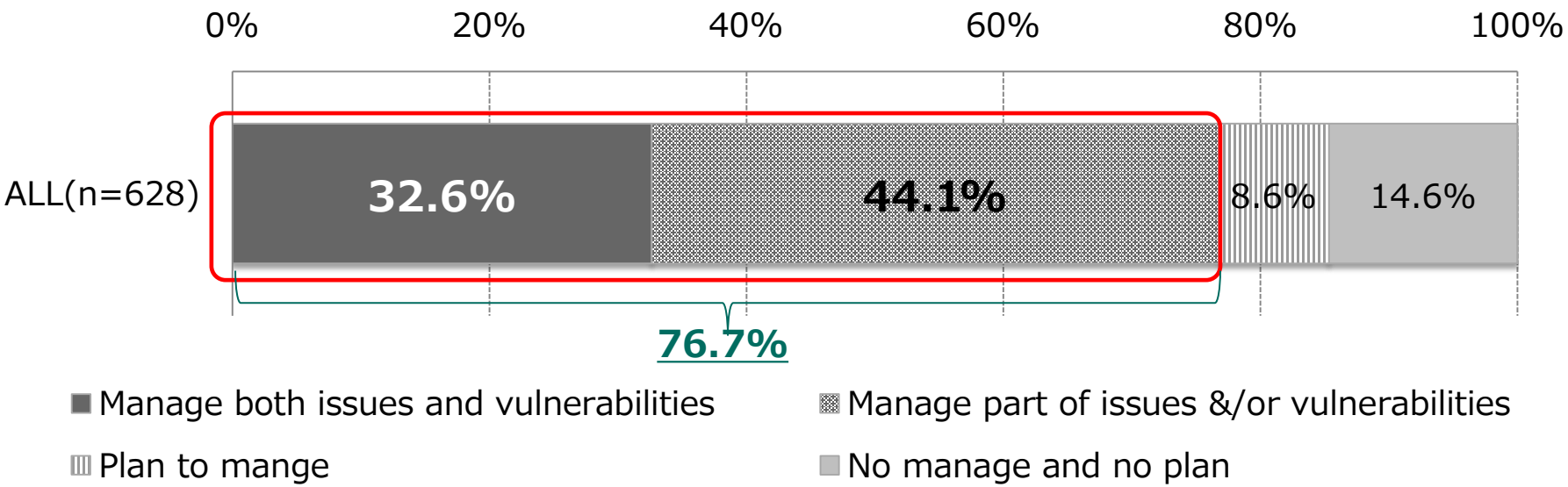
With regard to information classifications such as information to be kept confidential, information limited within the company, information which can be provided to the confidentiality agreement, publicly available information and etc. The table below shows the overall response status.

There were **48.2**% responded that “We have rules and classifies based on them.".

	Classify information assets		Not classify information assets	
Have documented rules	**1.execute (48.2%)**	2. not execute (5.1%)		
Not have documented rules	3.plan to document(3.8%)	4. no plan to document(7.7%)	5. plan to classify(6.7%)	6. no plan to classify(28.4%)

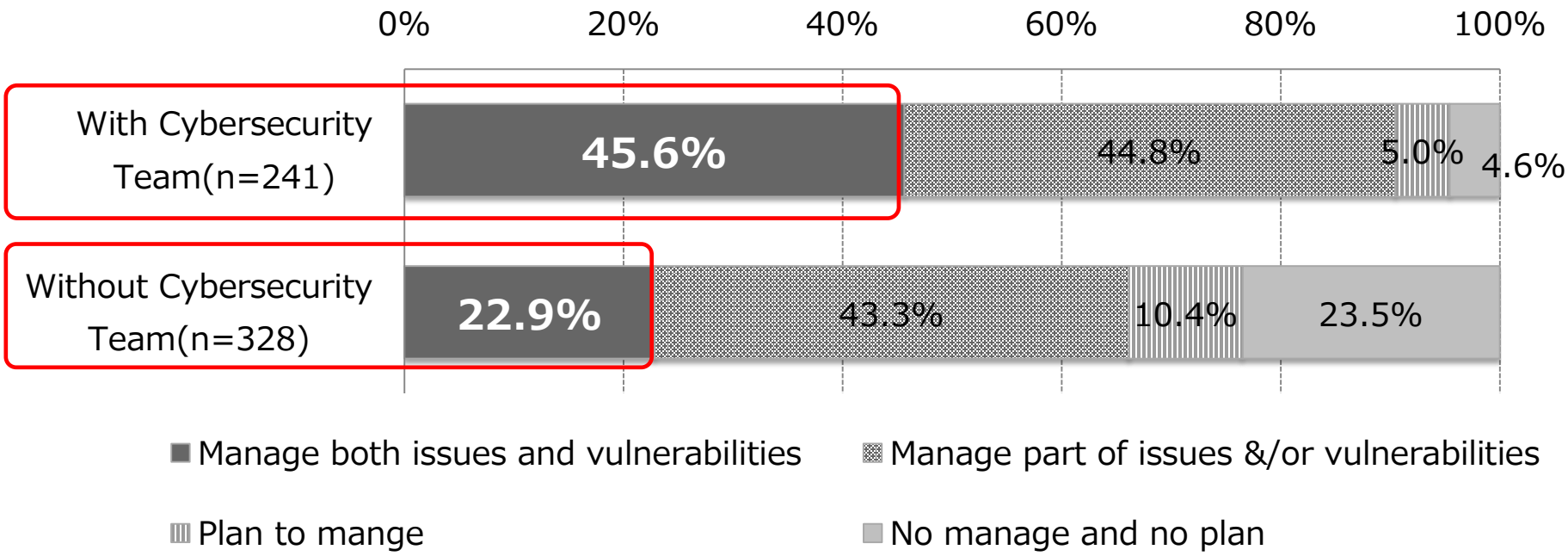
Issues and vulnerabilities of information assets

We confirmed the management status of the "problem and vulnerability of information assets" which we possess. **76.7%** answered that they are managing it. Although **32.6%** of respondents who answered that they are managing both issues and vulnerabilities.



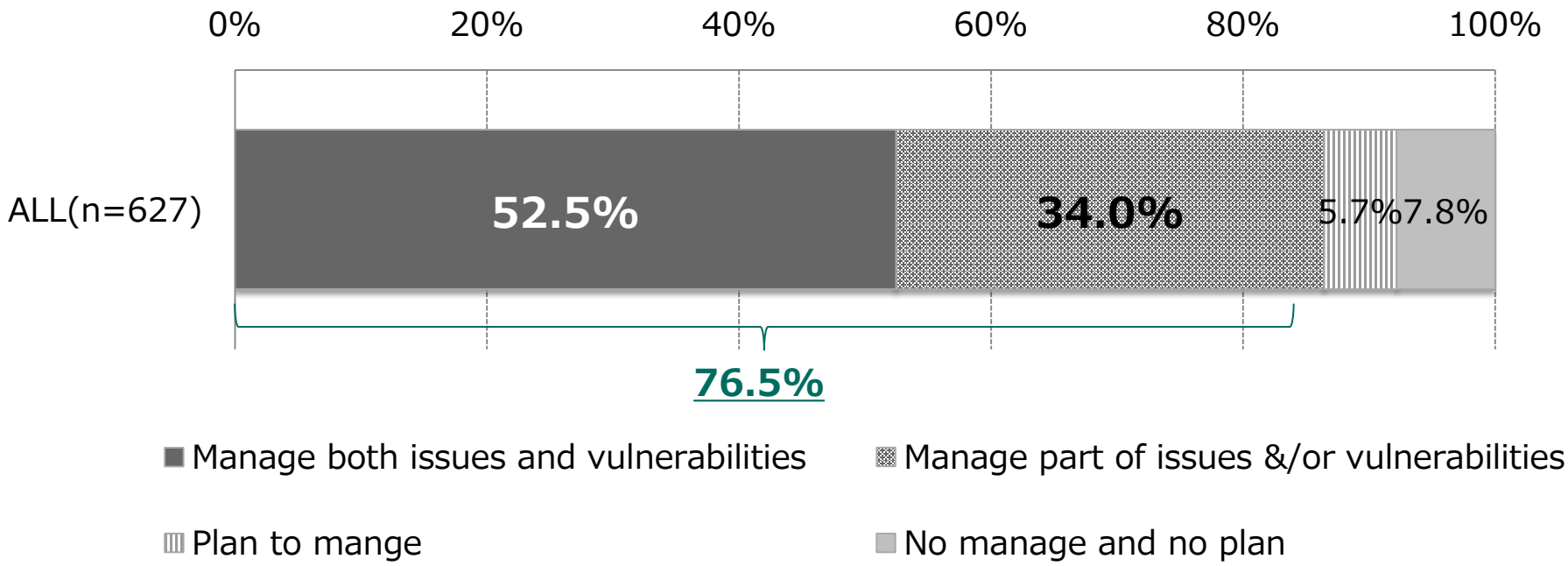
Issues and vulnerabilities of information assets

Separate the presence or absence of a company's cybersecurity team, ”Managing both issues and vulnerabilities” account for **45.6%** in companies with a cybersecurity team, while it is only **22.9%** in companies that do not have a team. There is a big difference depending on the presence or absence of a cybersecurity team.



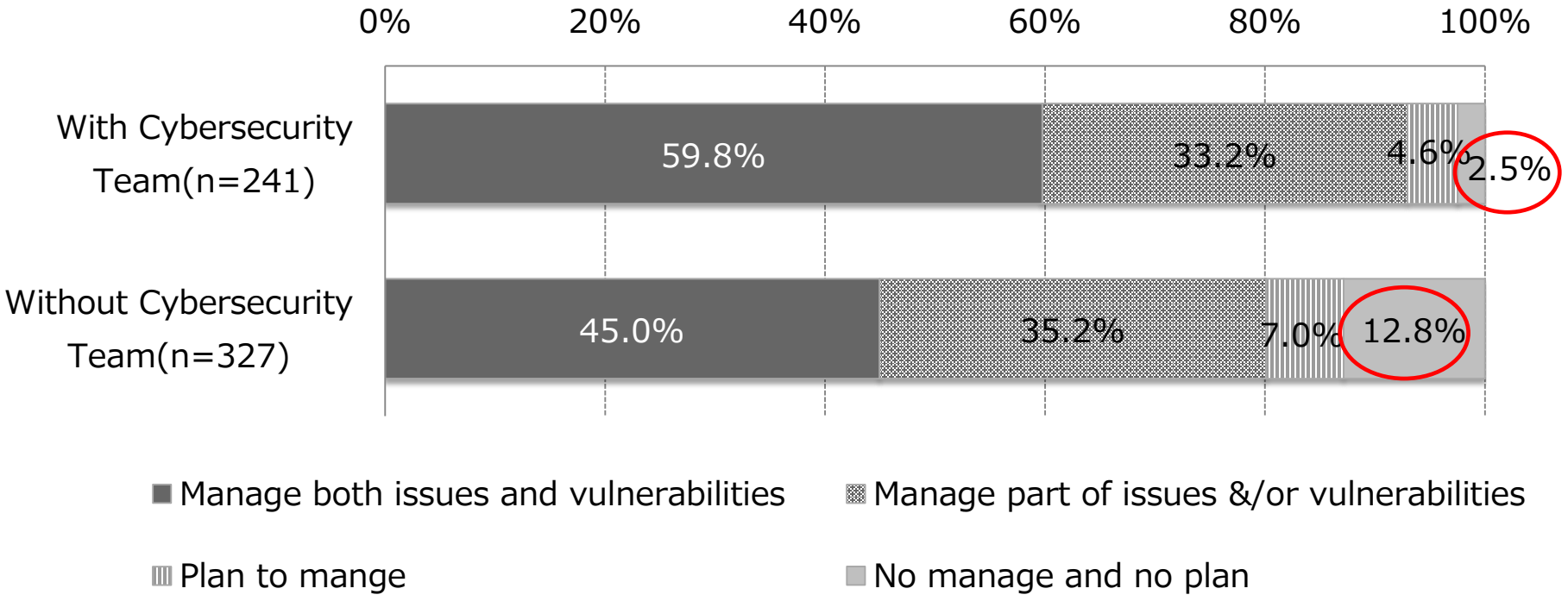
Issues and vulnerabilities in hardware asset management

We confirmed issues and vulnerabilities in hardware asset management. Overall, **76.5%** of companies replied that they are managing (total number of “Manage both issues and vulnerabilities” and “Manage part of issues &/or vulnerabilities”).



Issues and vulnerabilities in hardware asset management

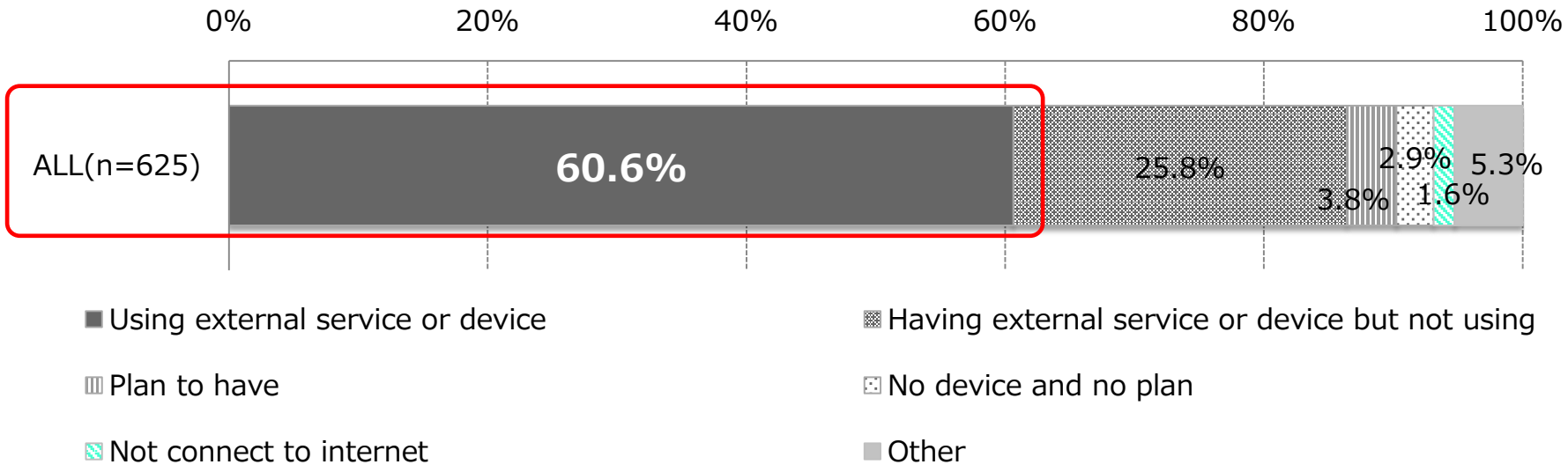
By separating the presence or absence of company's cybersecurity team, companies that responded "There is no plan (not planned)" are **2.5%** for companies with cybersecurity team, while **12.8**% for companies without cybersecurity team which shows there are large differences depending on whether or not the companies have a cybersecurity team.



Protect

Boundary defense between the Internet and its own network (ex. firewall)

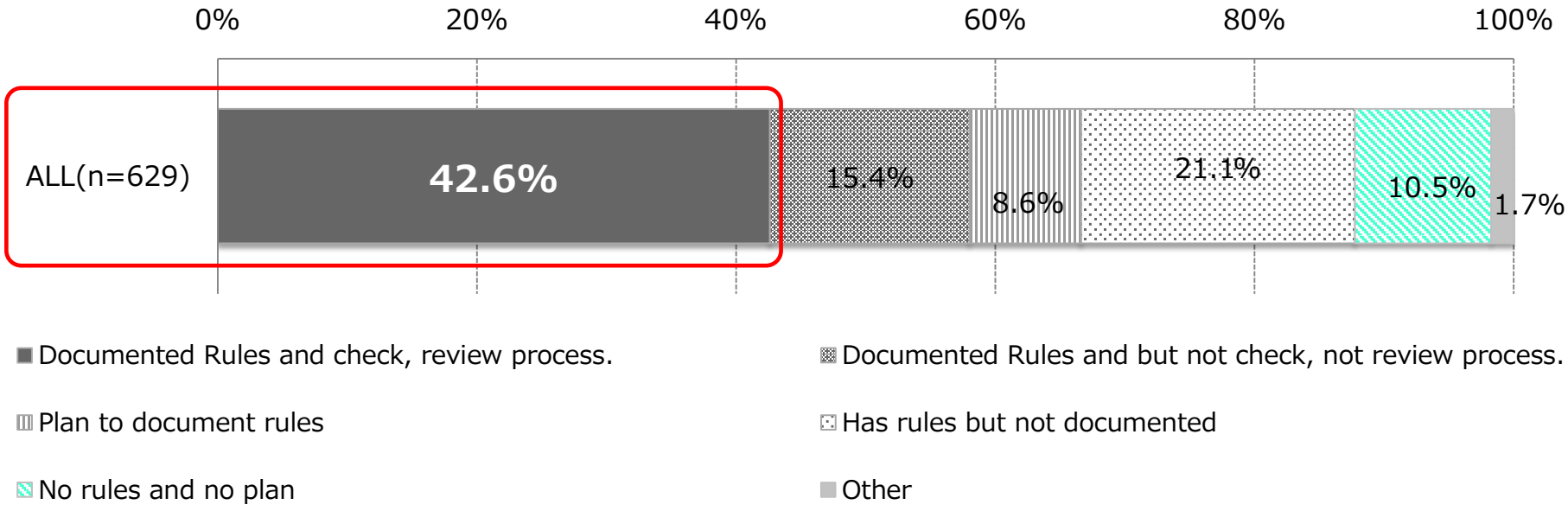
We confirmed the implementation status of the boundary defense between the Internet and its own network. **60.6%** of the companies chose “Using external service or device”.
In the “Other”, there were answers such as “Only subcontractor knows.” and etc..



Advancing with you
MS&AD
INSURANCE GROUP

Rules and formulation of user ID, password and authority for reference and update of information

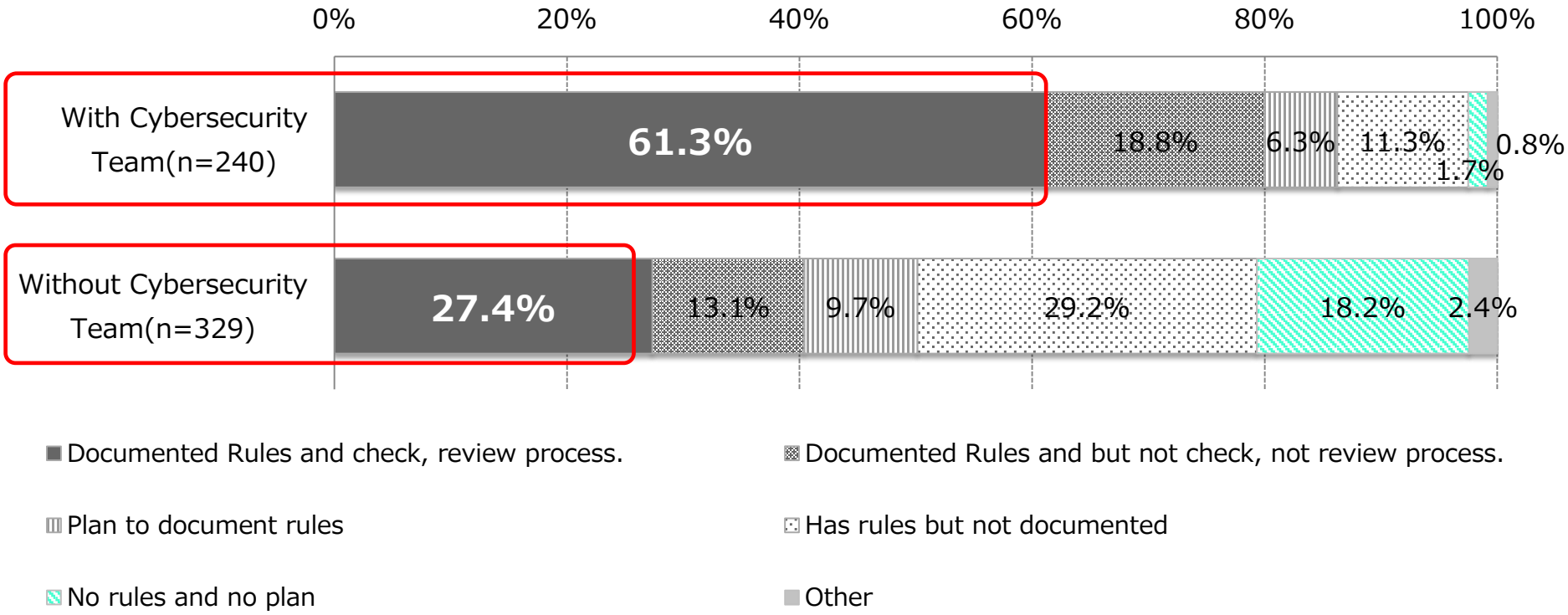
There are a majority (**42.6%**) of companies that responded the rules are documented and inspections and reviews are also being carried out.
In the “Other”, there were answers such as “No rules but check , review process.”, "conforms to the rule/management of the parent company“ , and etc..



Advancing with you
MS&AD
INSURANCE GROUP

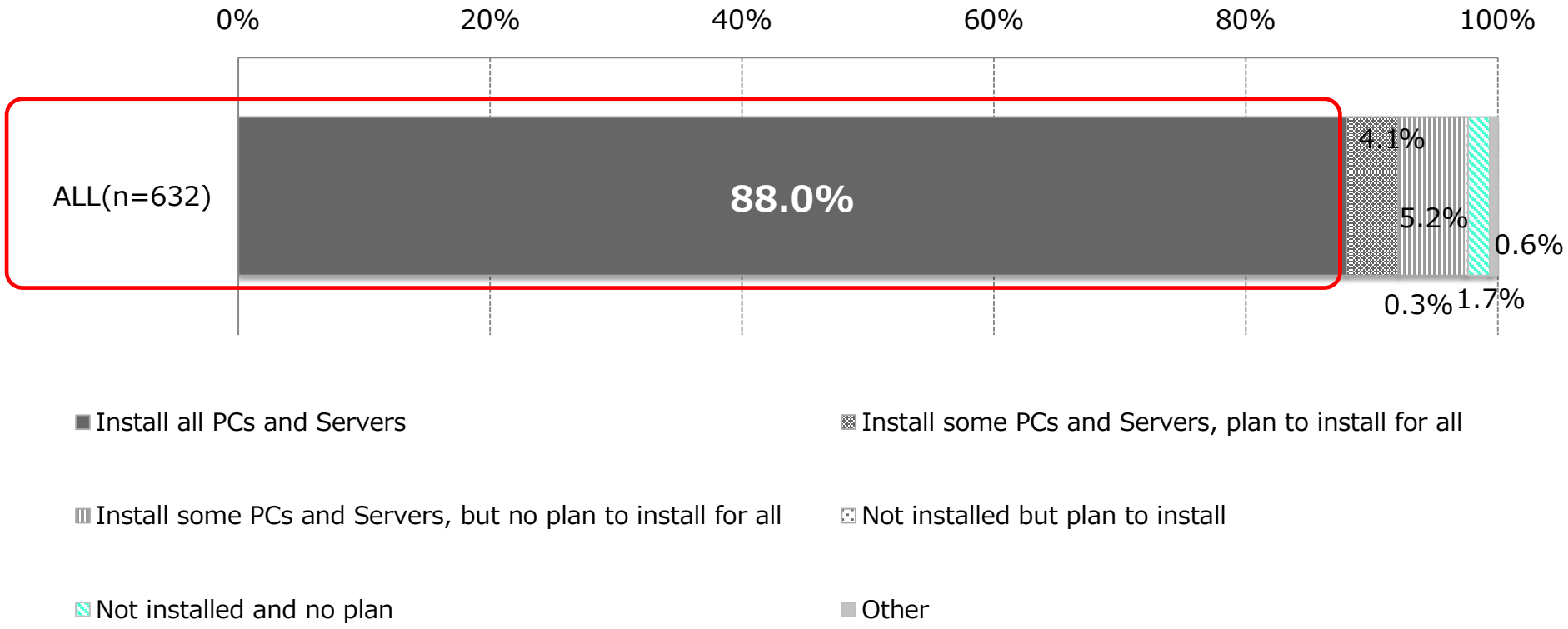
Rules and formulation of user ID, password and authority for reference and update of information

61.3% for companies with cybersecurity team and **27.4%** for companies without a cybersecurity team, which is more than 33 points away.



Status of antivirus/antimalware software

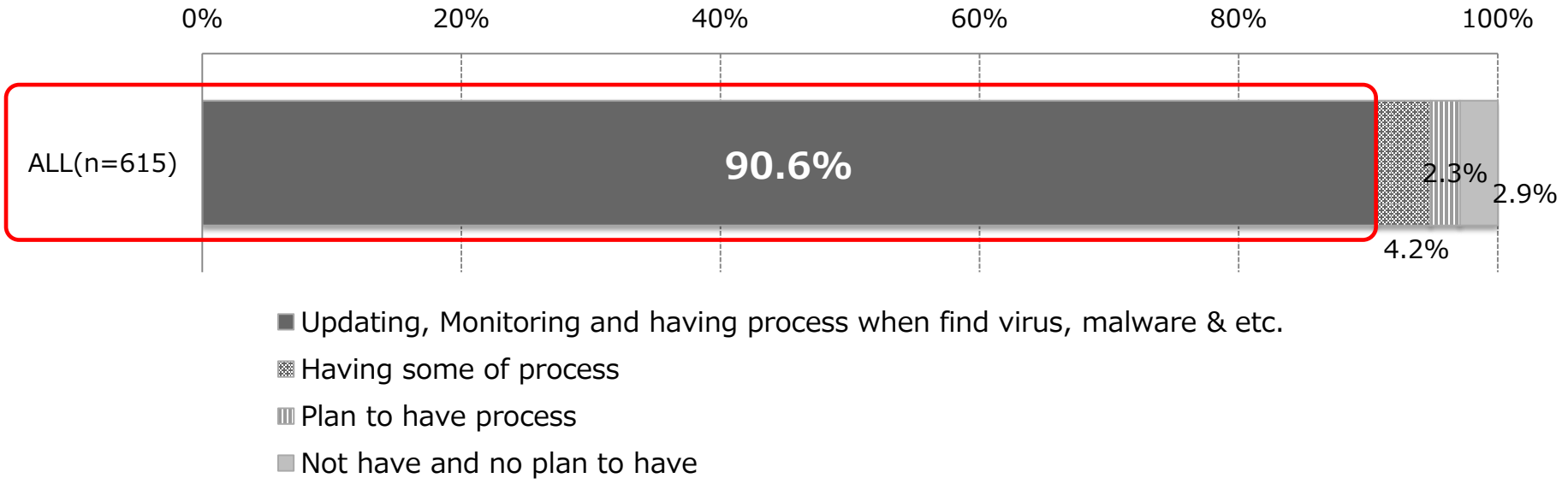
There are **nearly 90%** of companies that replied: “installed on all PCs & servers".
In addition, "Other", there was a reply that it is being implemented by the subcontractor.



Status of updating/monitoring of software

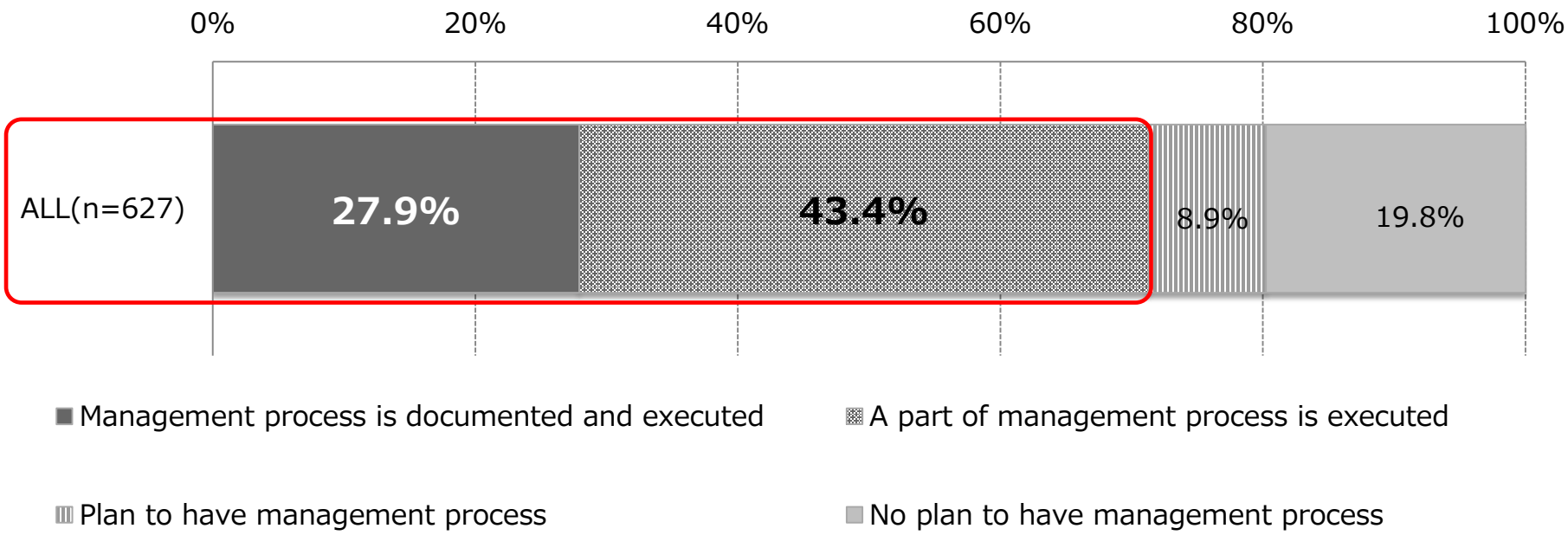
(Only install in the previous question)

More than 90% of respondents are ”Update, monitoring and having a process when finding vírus, malware & etc.".



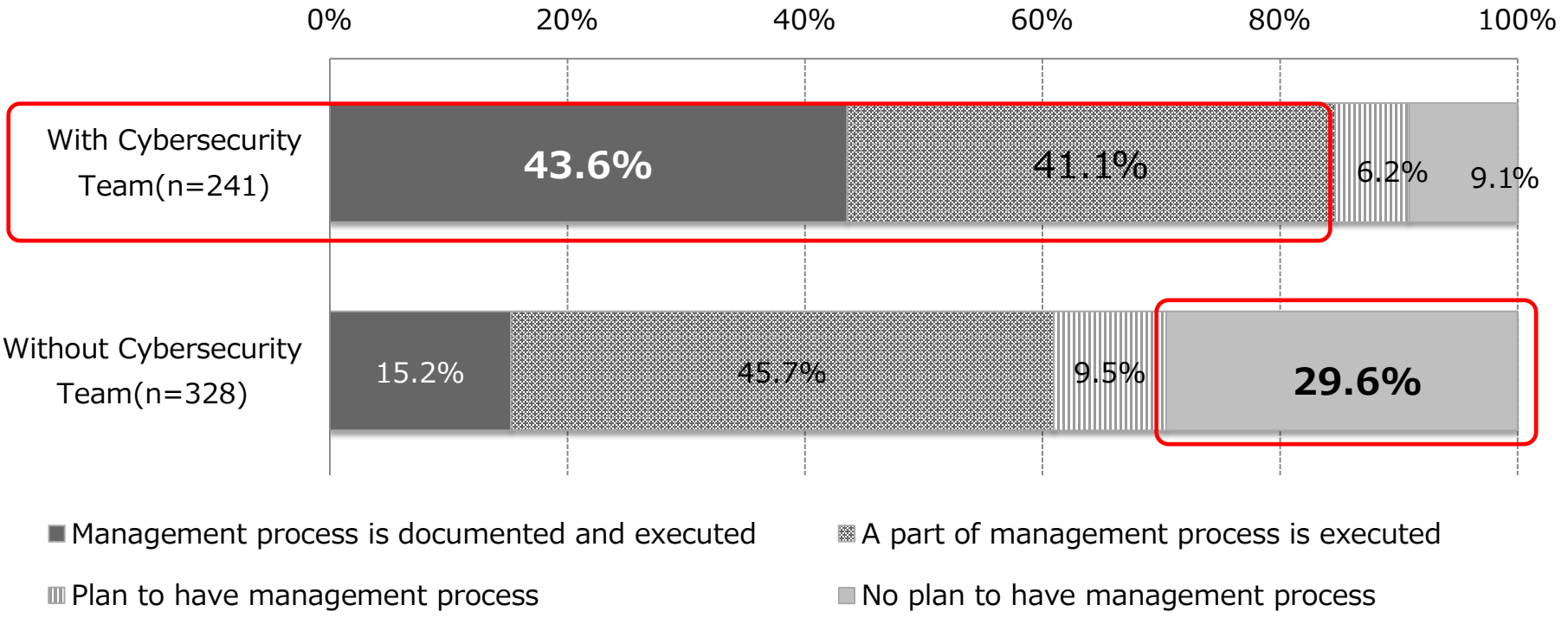
Status of vulnerability management (ex. Windows update)

Considering that ”Implemented & documented management methodology" and "conducting partly" together, more than **70% of companies are managing their vulnerabilities**. However, less than 30% of the respondents are documented their methodologies.



Status of vulnerability management (ex. Windows update)

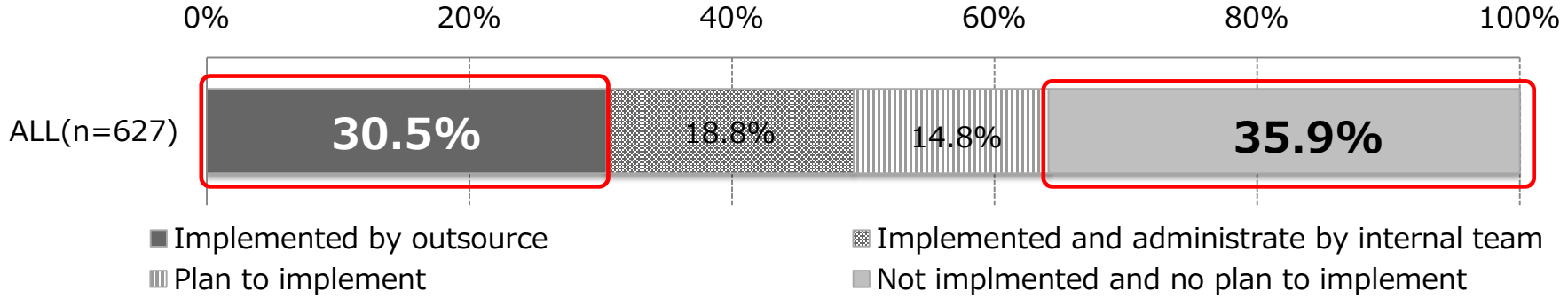
Companies with cybersecurity team achieved **43.6%** for "Implemented & documented management methodology" and more than **80%** are managing vulnerability. On the other hand, **29.6%** of companies without a cybersecurity team are "No plan to have management process".



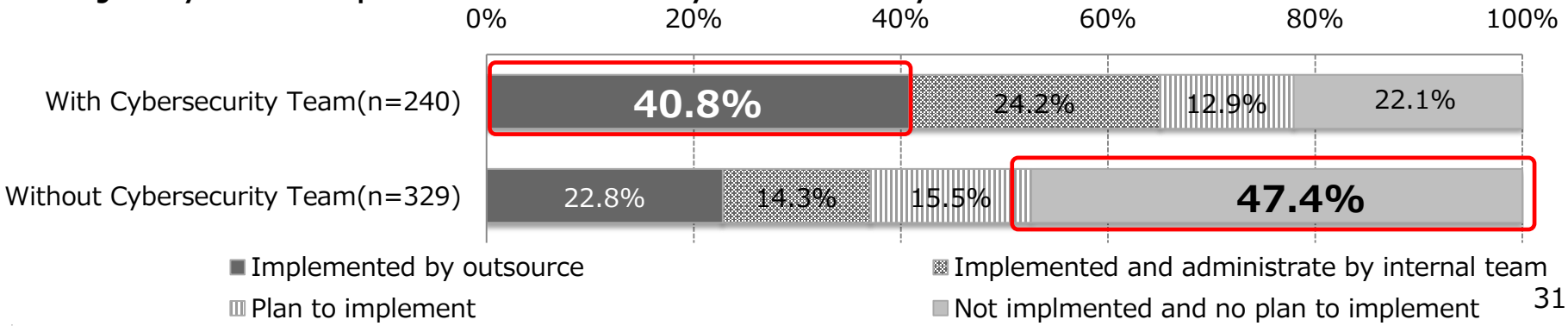
Detect

Security monitoring systems implementation status ex) IDS and IPS

The largest majority is ”Not implemented and no plan" (**35.9%**), then ”Implemented by outsource" (**30.5%**) comes second.

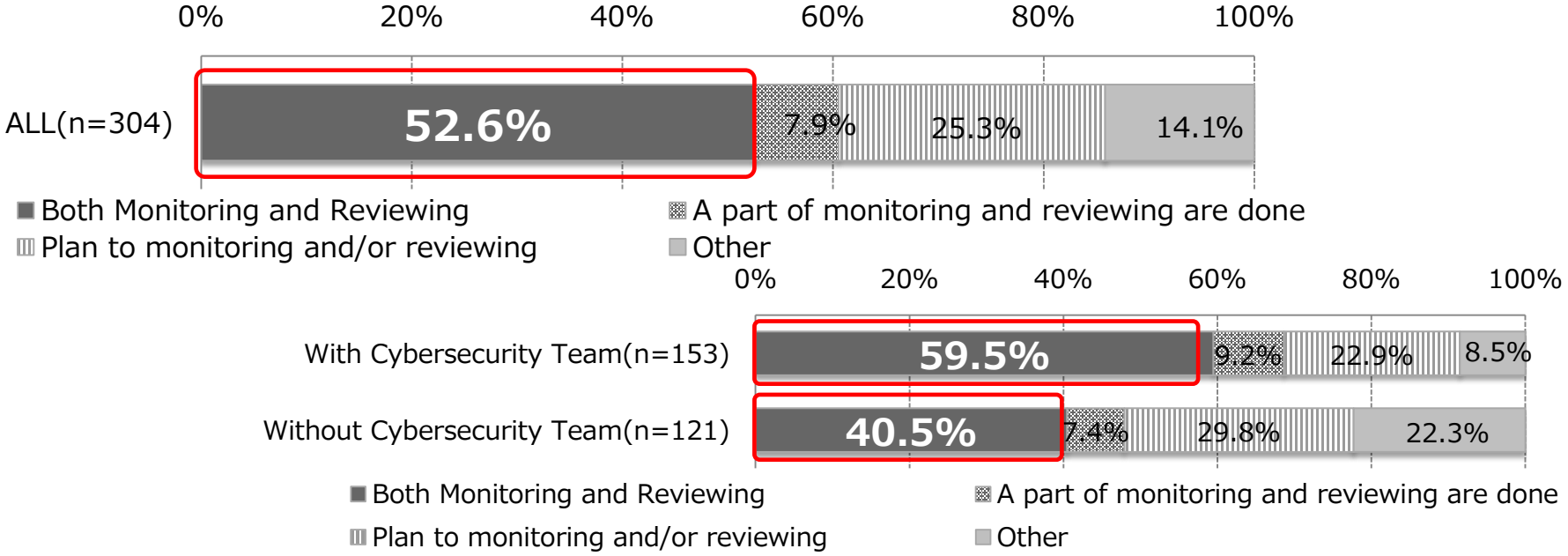


Compare by with or without a cybersecurity team, it is higher for “Implemented by outsourcing“ (**40.8%**) for companies with cybersecurity team. But on the other hands, “Not implemented and no plan” (**47.4%**) is a majority of companies without cybersecurity team.



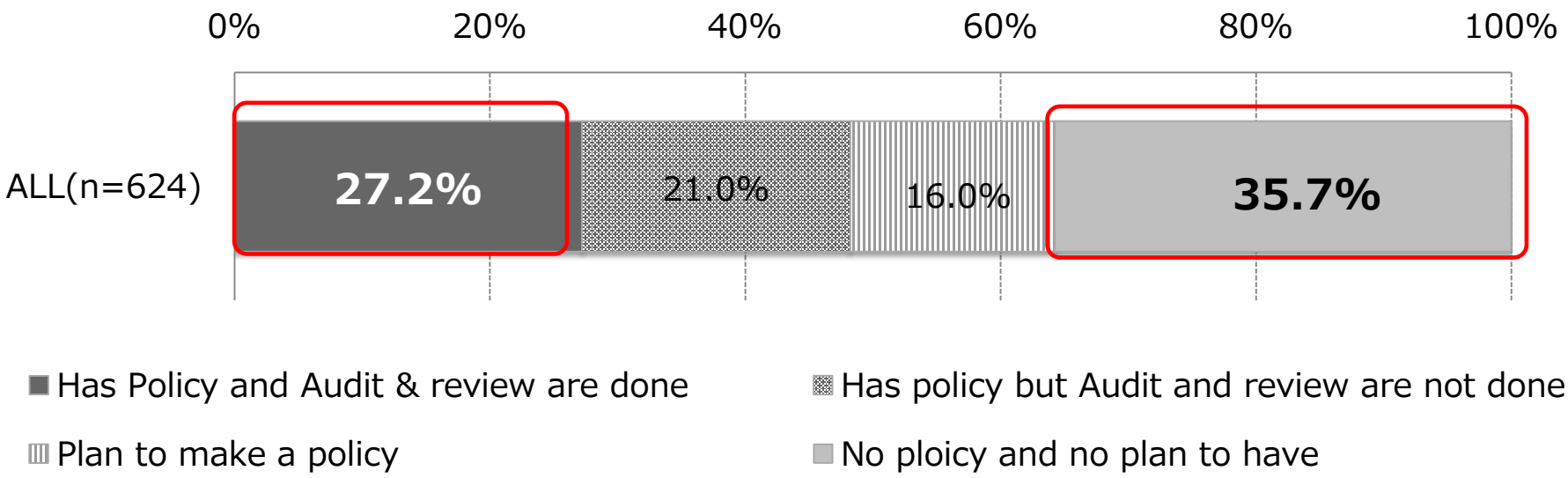
Audit of security monitoring systems and define processes for incidents.

"Both monitoring and reviewing" is a majority (**52.6**%) of the respondents.
Compare by with or without a cybersecurity team, there is a huge difference (19.0points) between. (With:**59.5**%, Without:**40.5**%)
In the "A part of monitoring and reviewing are done", there were answers such as "Only Monitoring.", "conforms to the rule/management of the parent company" , and etc..
In the "Other", there were answers such as "Outsourcing", and etc..



Policy for system logs

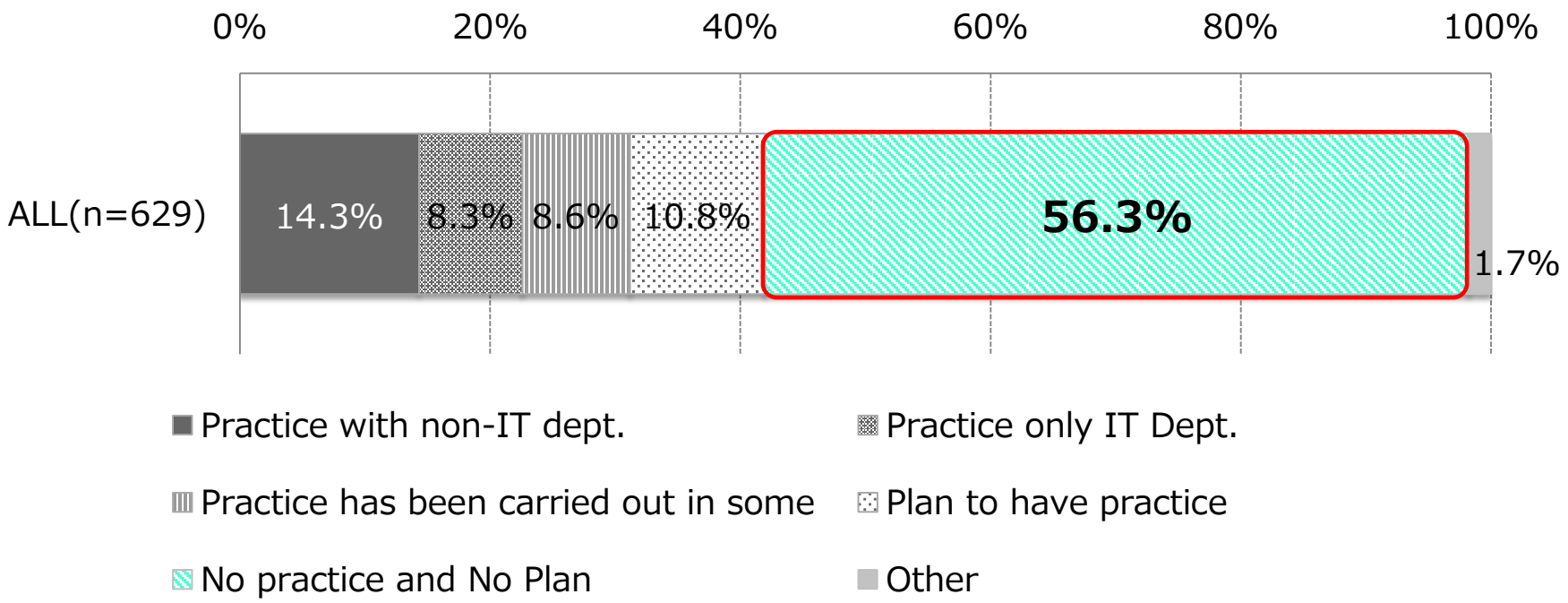
The largest majority is “No Policy and no plan “ (**35.7%**). But on the other hands, “Has Policy and Audit & review are done” (**27.2%**) is in the second majority.



Respond & Recover

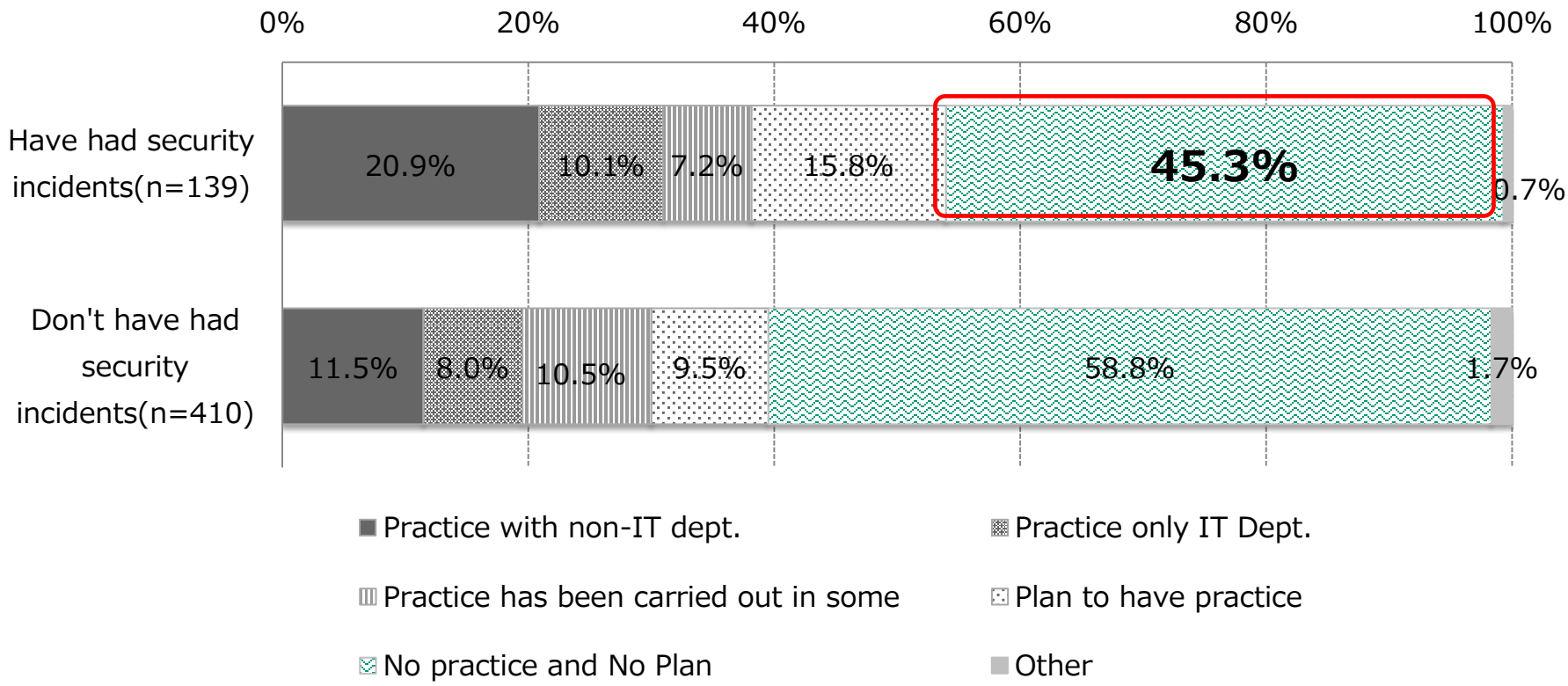
Training for the security incidents occur

More than half (**56.3%**) are responded “No practice and no plan”.
In “Other”, we received the answer like; “Order from a parent company”, “Training is conducted by each department.” and so on.



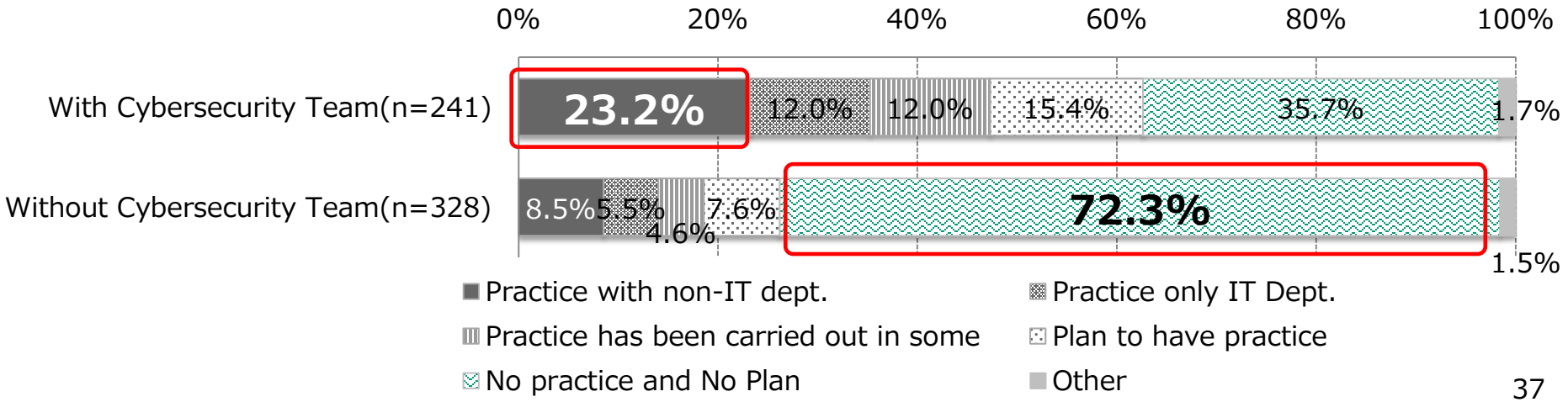
Training for the security incidents occur

Compare by have or don't have had security incidents, **More than 40%** of companies , have had security incidents, choose "No practice and No Plan".



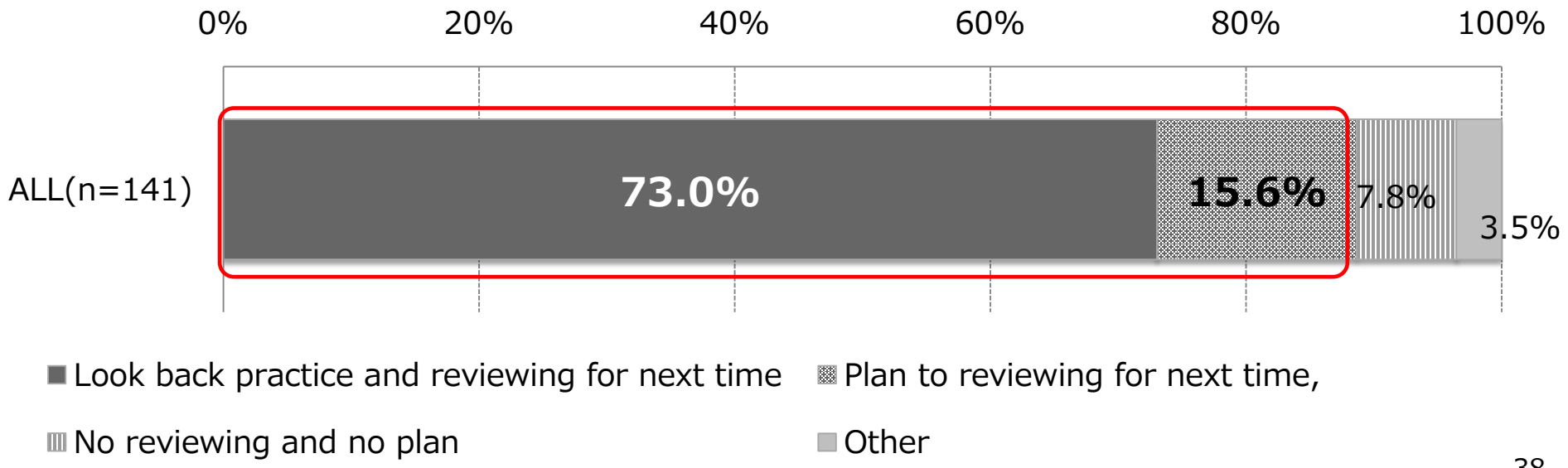
Training for the security incidents occur

It is higher for “Practice with non-IT dept.“ (**23.2%**) for companies with cybersecurity team. But on the other hands, “No practice and No Plan” (**72.3%**) is a majority of companies without cybersecurity team.
In companies with cybersecurity team, the detection of alerts while protecting cyber security can lead to accident detection and response, and it is considered that accidents, including minor accidents, can be dealt with at a time when the scope of impact is small while judging the situation. For companies that do not have cybersecurity team or have a small workforce, it is necessary to outsource the ability to handle potential cybersecurity incidents when the impact is small.



Review of “Training for the security incidents occur”

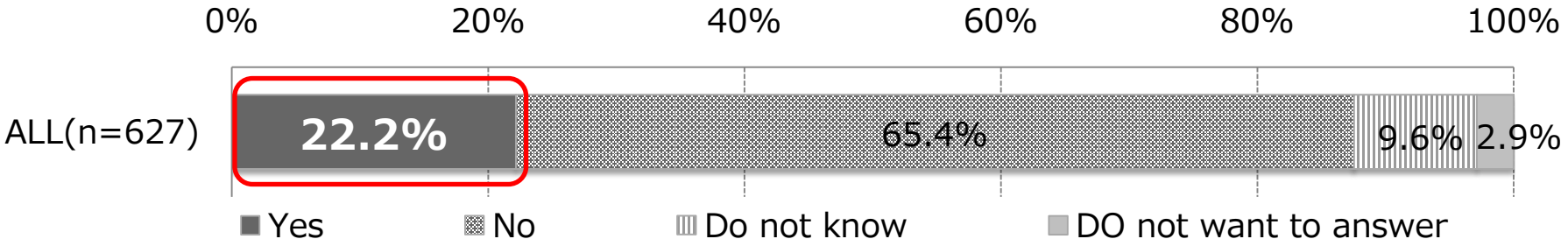
73.0% of respondents are ”Look back practice and reviewing for next time”. And including who has the plan to review, it is close to 90%. It means most of the companies who have practice/training are reviewing/plan to review.
In “Other”, we received the answer like;” Training is conducted by the parent company“、”We don't feel the need to review the training.“and so on.

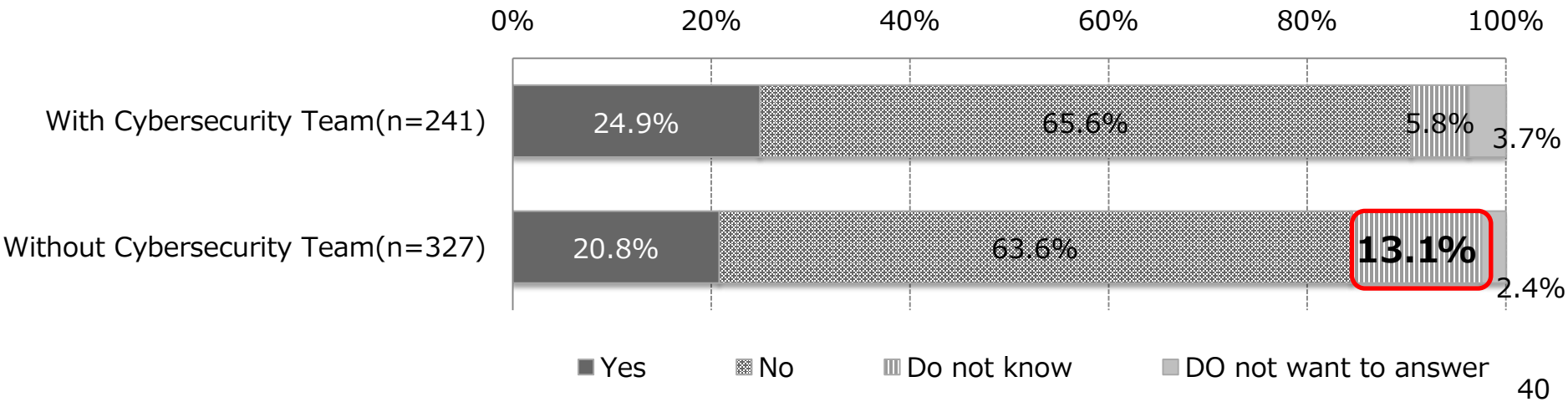


Security incidents

Occurrence of cyber security incidents

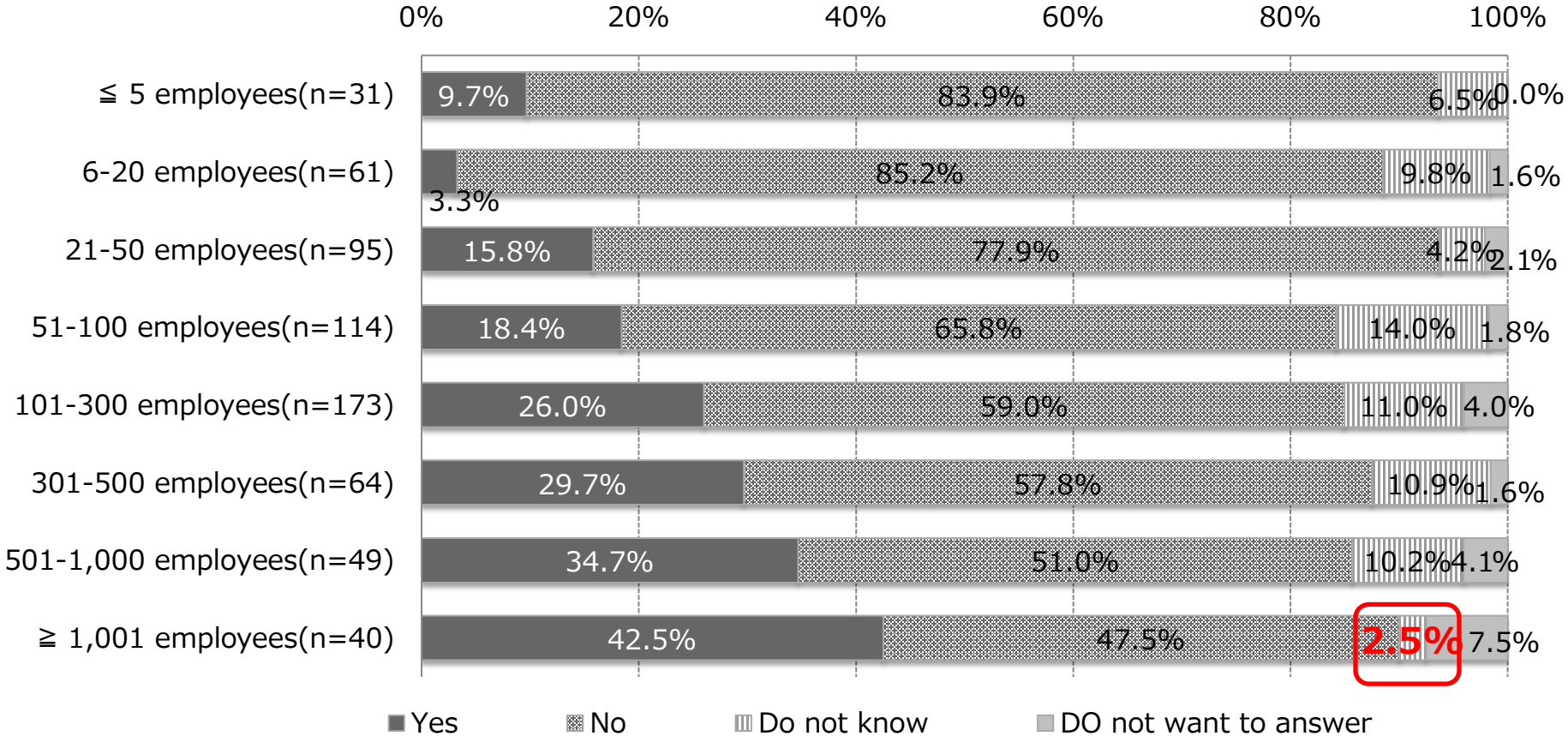
Answering to the question that they had a cybersecurity incident in the past, **22.2%** of companies said "Yes".
13.1% of companies without a cybersecurity team answered as “No not know”. They might not be aware of security incidents.





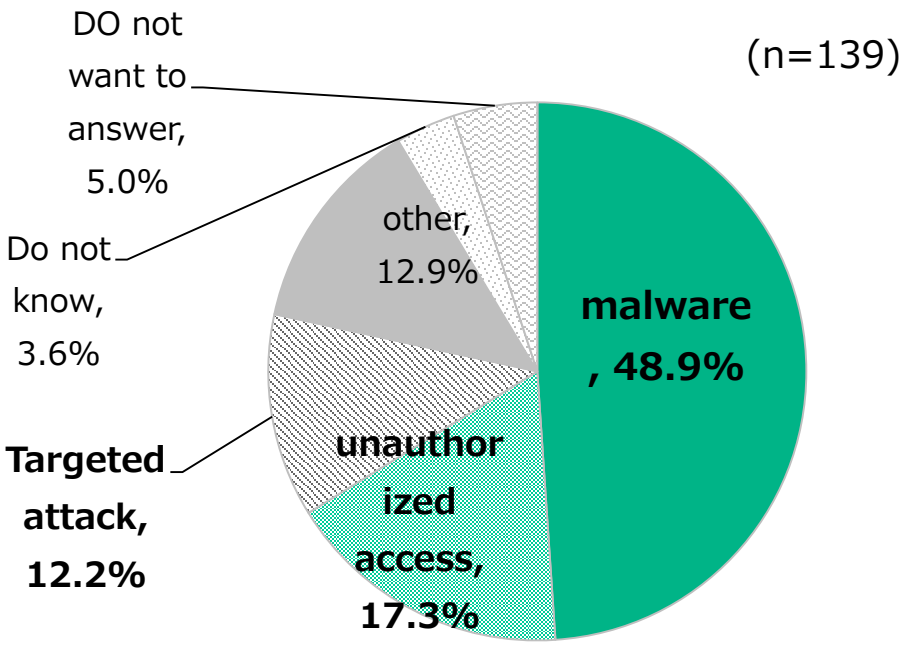
Occurrence of cyber security incidents

The result of research for enterprises with 1,001 or more is clearly small (2.5%) for “Do not know.", while the same for less than 1,000 employees enterprises are very high.



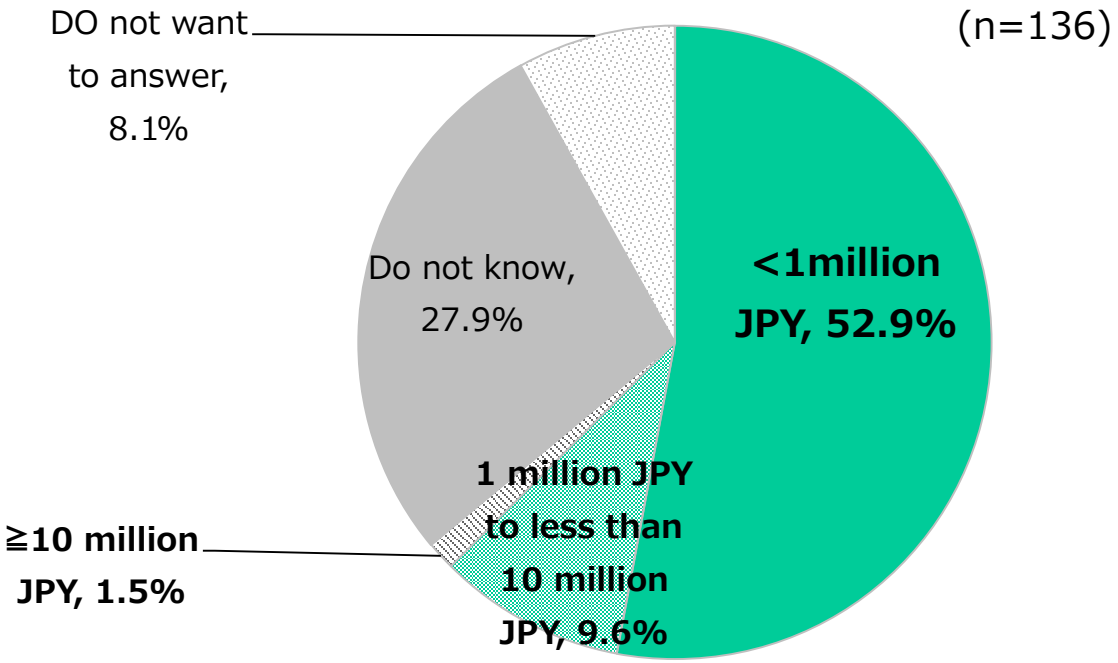
Details of the most serious incident

What caused the biggest damage by the cyber incidents are as follows:
1st: Malware (**48.9%**), 2nd: unauthorized access (**17.3%**) and
3rd: Targeted attack (**12.2%**).
In “Other”, we received the answer like; ”inside job“, ”Business E-mail Compromise (BEC)“ and so on.



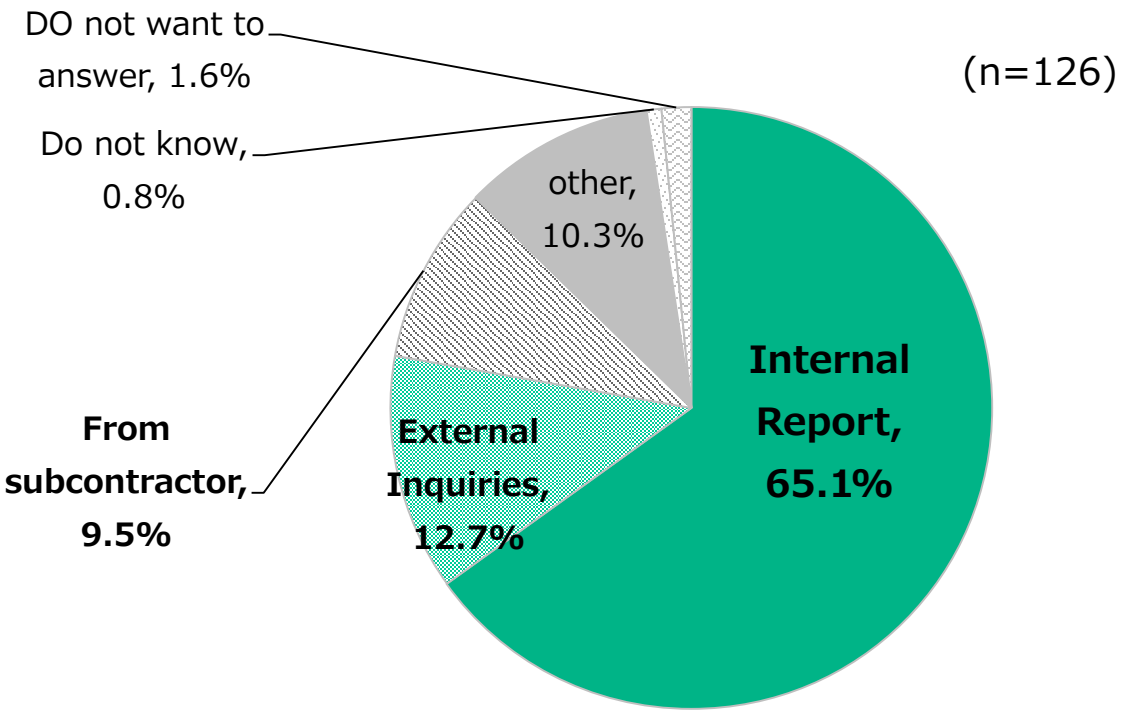
maximum amount of damage

When we confirmed the amount of damage from the most serious incident, the results were as follows:
1st: under 1million JPY (**52.9%**), 2nd: 1 million to 10 million JPY (**9.6%**), and 3rd: 10 million yen or more (**1.5%**).



Reason for recognizing the incident

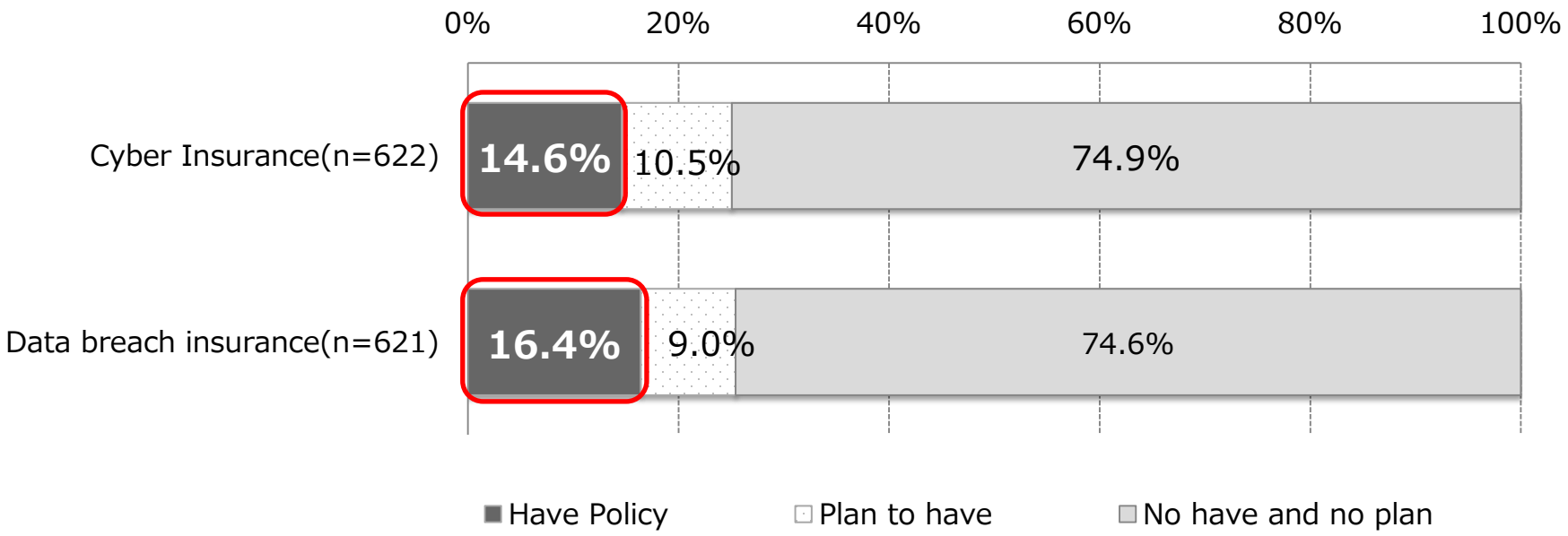
“How the enterprise recognized the accident?”.
The results were as follows:
1st: Internal Report (**65.1%**), 2nd: External Inquiries (**12.7%**), and
3rd: From subcontractor (**9.5%**).
“Other” contains ”System detection“, ”Parent company’s report“ and so on.



Cyber insurance

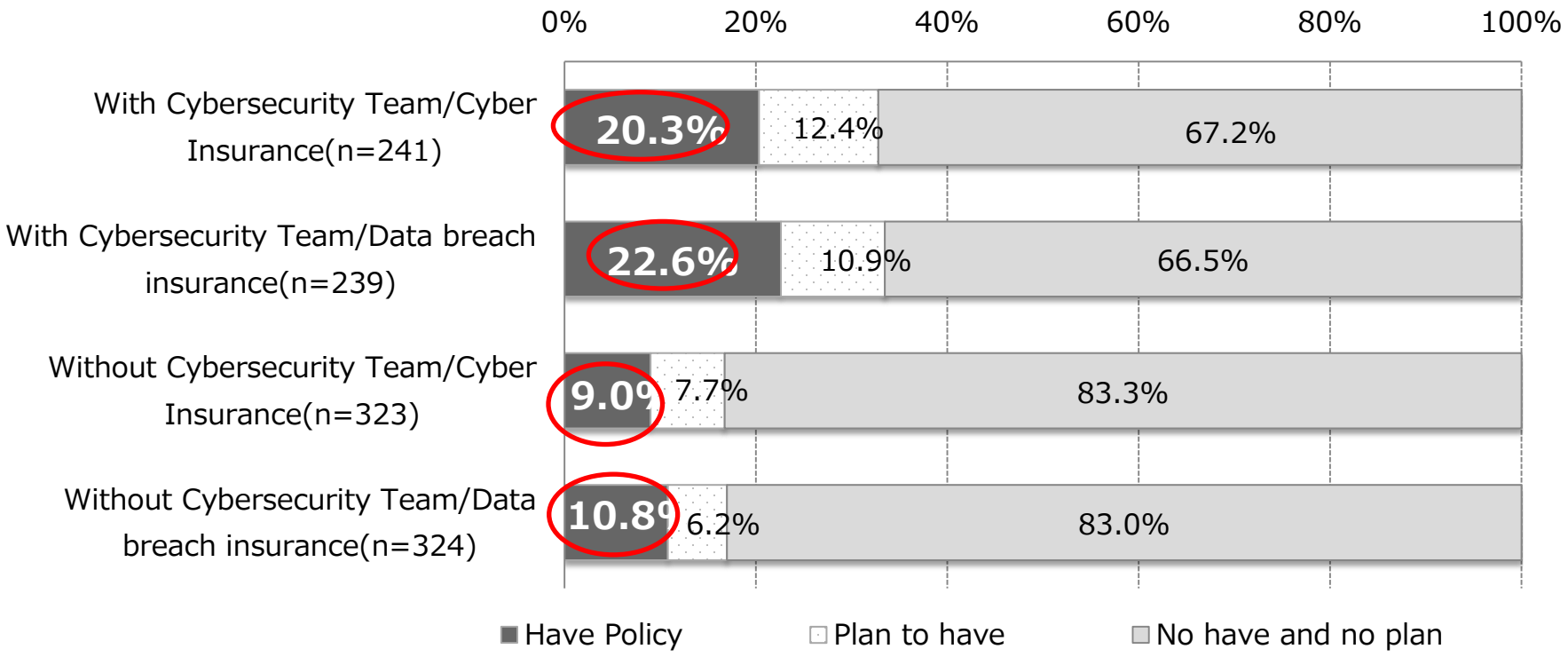
Status of cyber insurance & data breach insurance

"Not have and no plan" achieved more than 70% for both insurances. It is only **14.6%** for cyber insurance and **16.4%** for data breach insurance who have a policy.



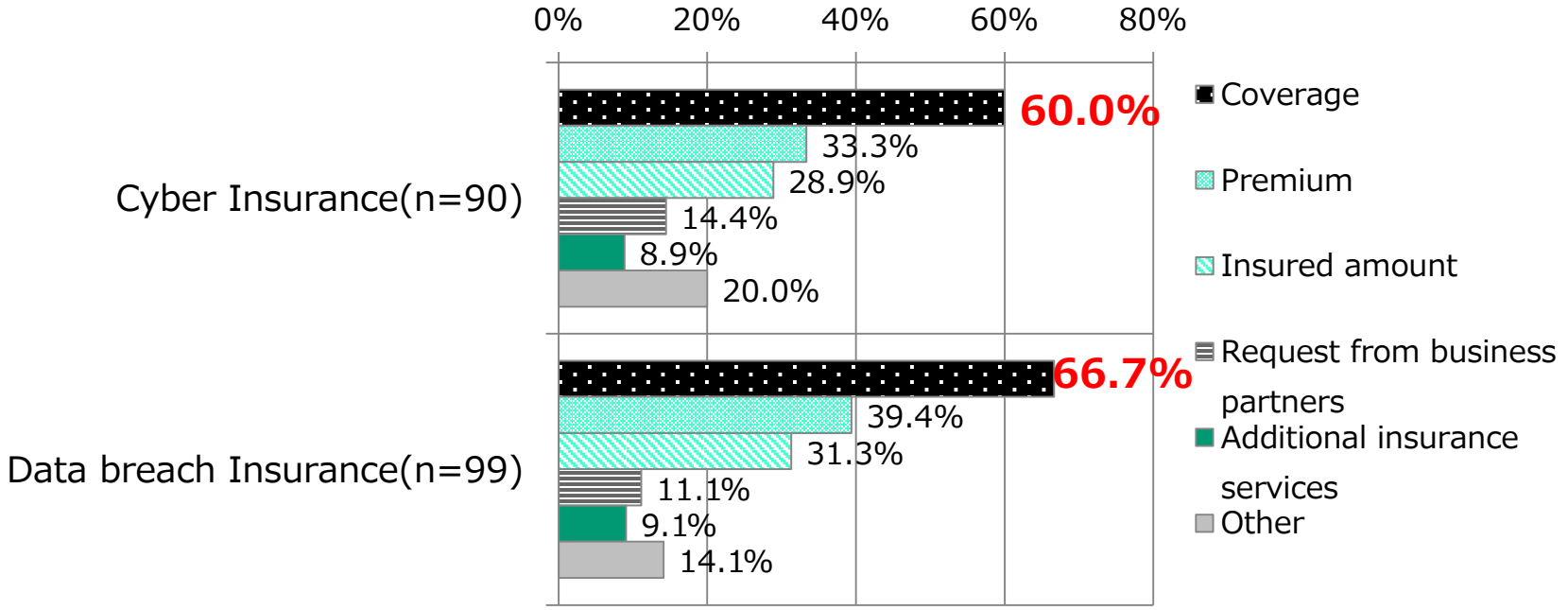
Status of cyber insurance & data breach insurance

Compare by with or without of cybersecurity team, it is **20.3%** "with cybersecurity team" who has cyber insurance policy which is **9.0%** "without". (More than two times). For data breach insurance, the situation seems the same as "with" is **22.6**% and "without" is **10.8**%.



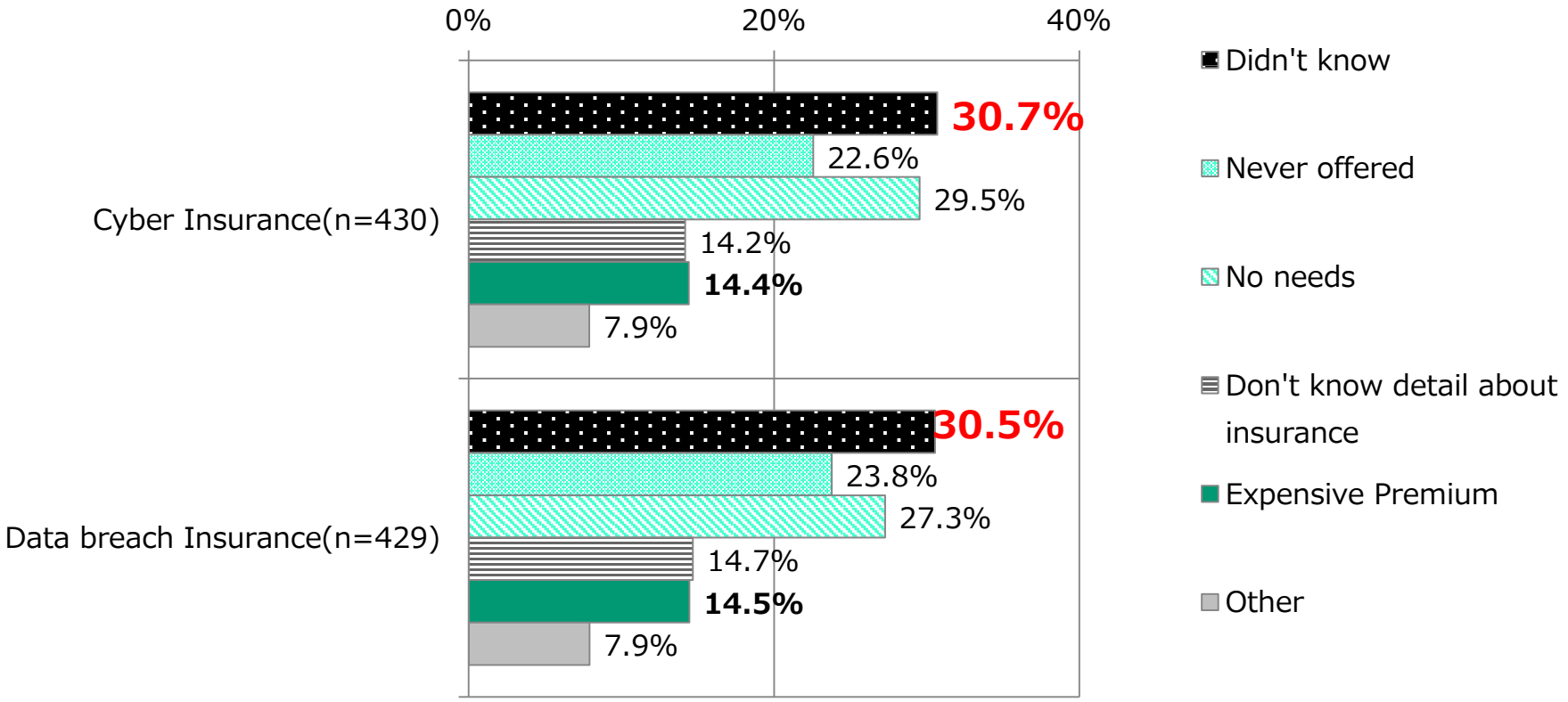
The reason who have policy *multiple answer

The most common reason for buying insurance was “**Coverage** ” （**Cyber Insurance : 60.0%、Data breach Insurance : 66.7%**）。
“Other” contains “blanket insurance”, “Request from the parent company and/or head office”, and etc..



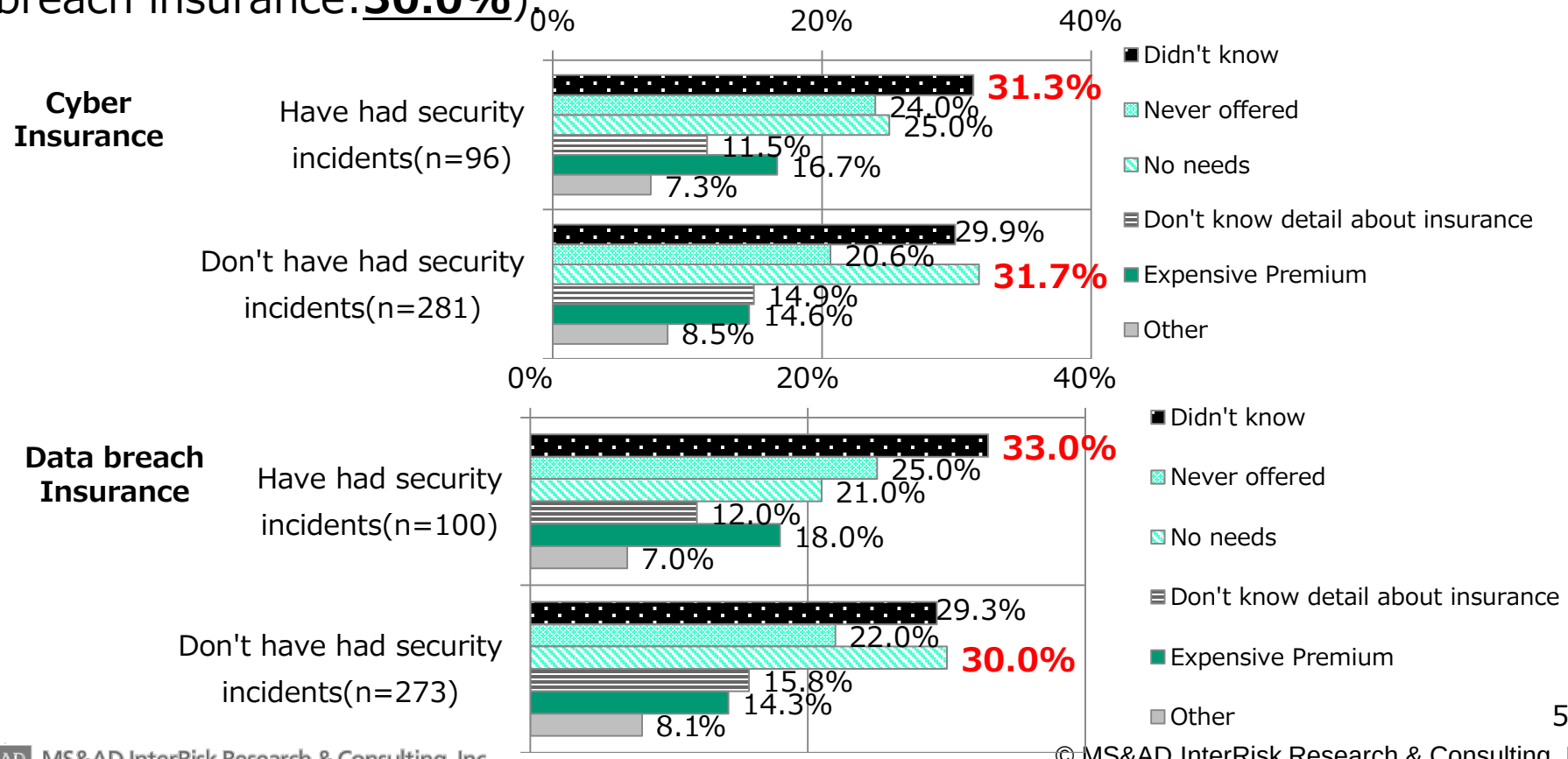
The reason who don't have policy *multiple answer

The Majority is "Didn't know about the insurance" (Cyber insurance: **30.7%**, Data breach insurance: **30.5%**) and the reason is **not** by "Expensive premium".



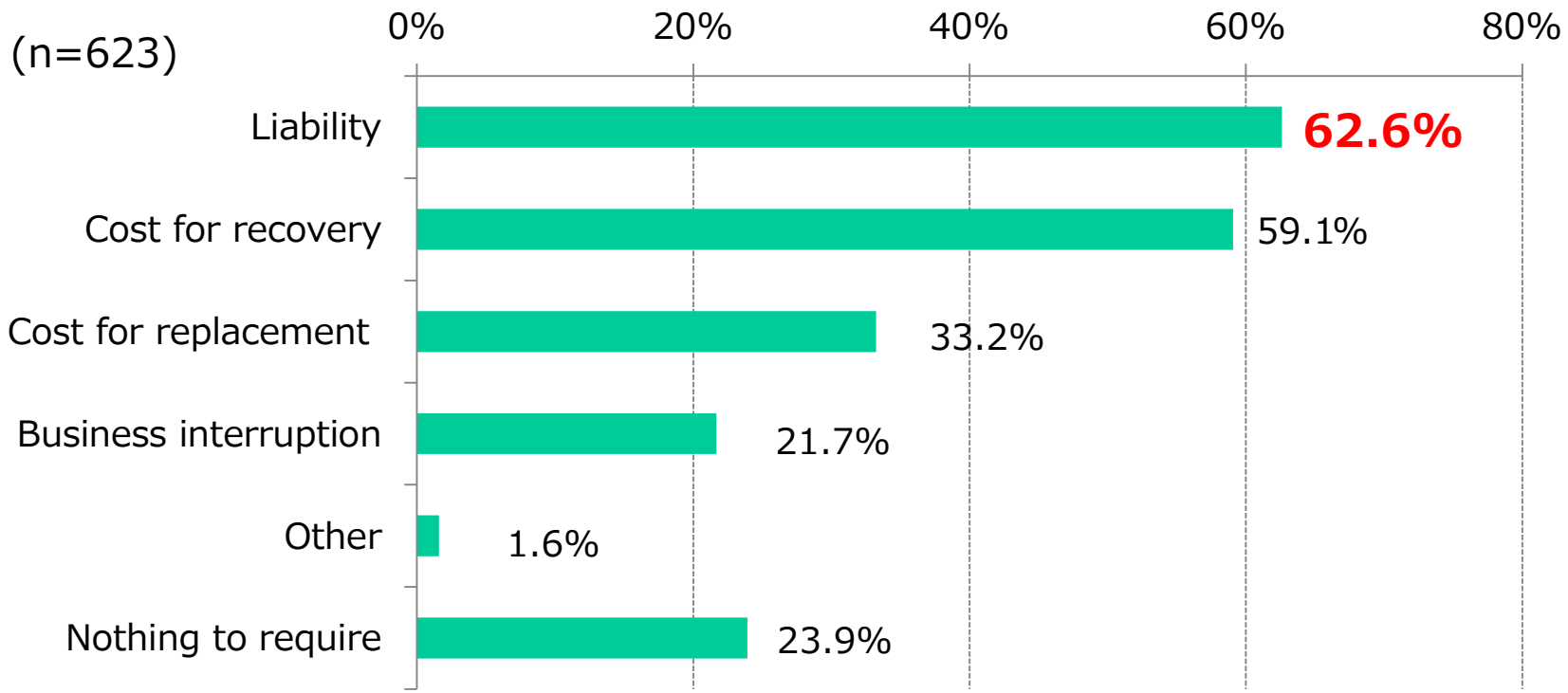
The reason who don't have policy *multiple answer

While the majority of companies that have experienced security incidents said, "Didn't know"" (Cyber insurance:**31.3%** and Data breach insurance:**33.0%**), the majority of companies that have not experienced security incidents said, "No needs" " (Cyber insurance:**31.7%** and Data breach insurance:**30.0%**).



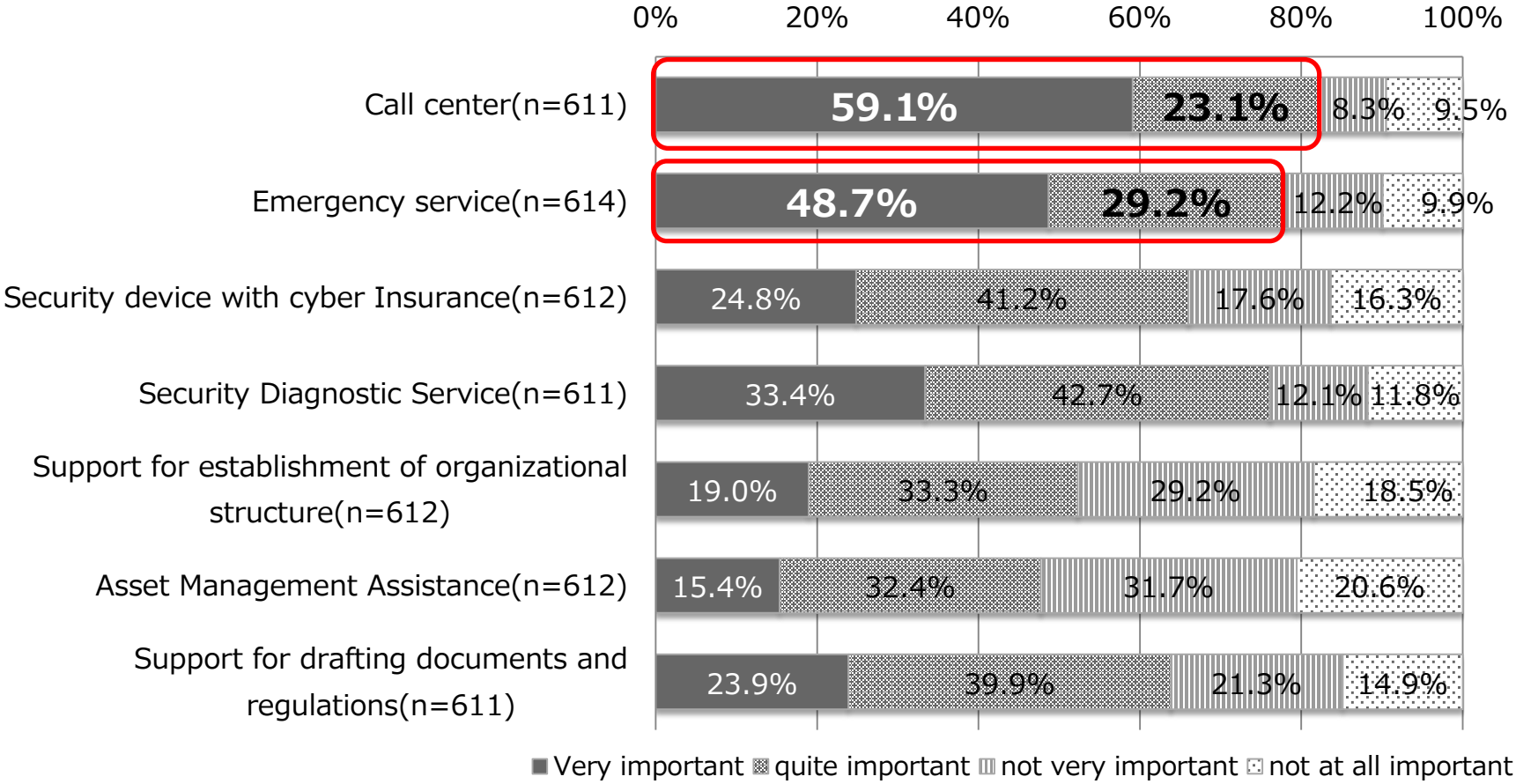
Required coverage *multiple answer

The majority of the answer is "**Liability (62.6%)**" and for the second, **"Cost for recovery(59.1%) "** .
In the "Other", there were answers such as " Expenses paid to lawyers who provided support for the handling of the mass media",and etc..



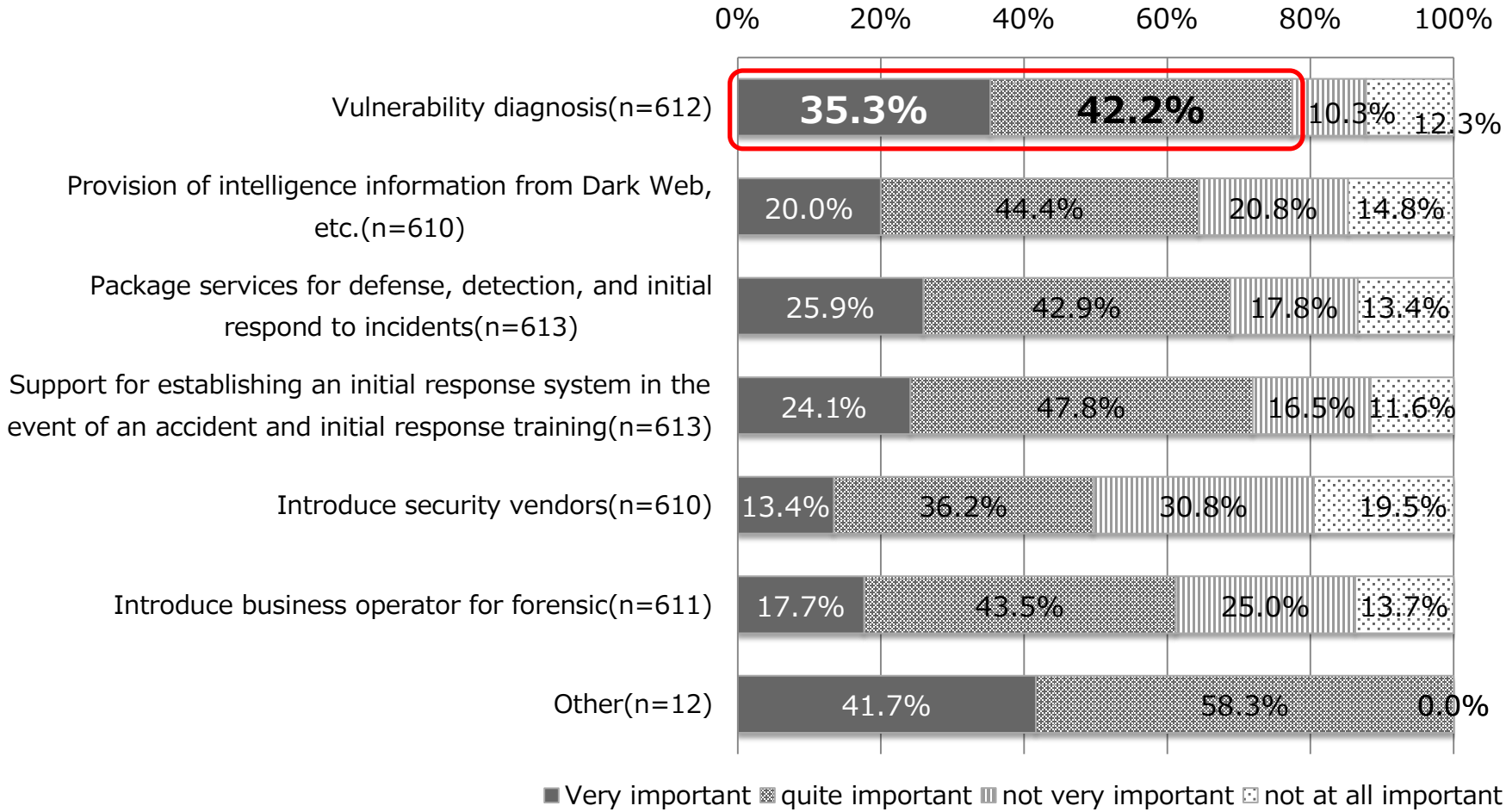
Expectations for additional insurance services(1/2)

When we checked expectations for additional insurance services, the results were as follows: 1st: Call center (**82.4%**), 2nd: Emergency service (**77.9%**) and 3rd: Vulnerability diagnosis (**77.5%**).



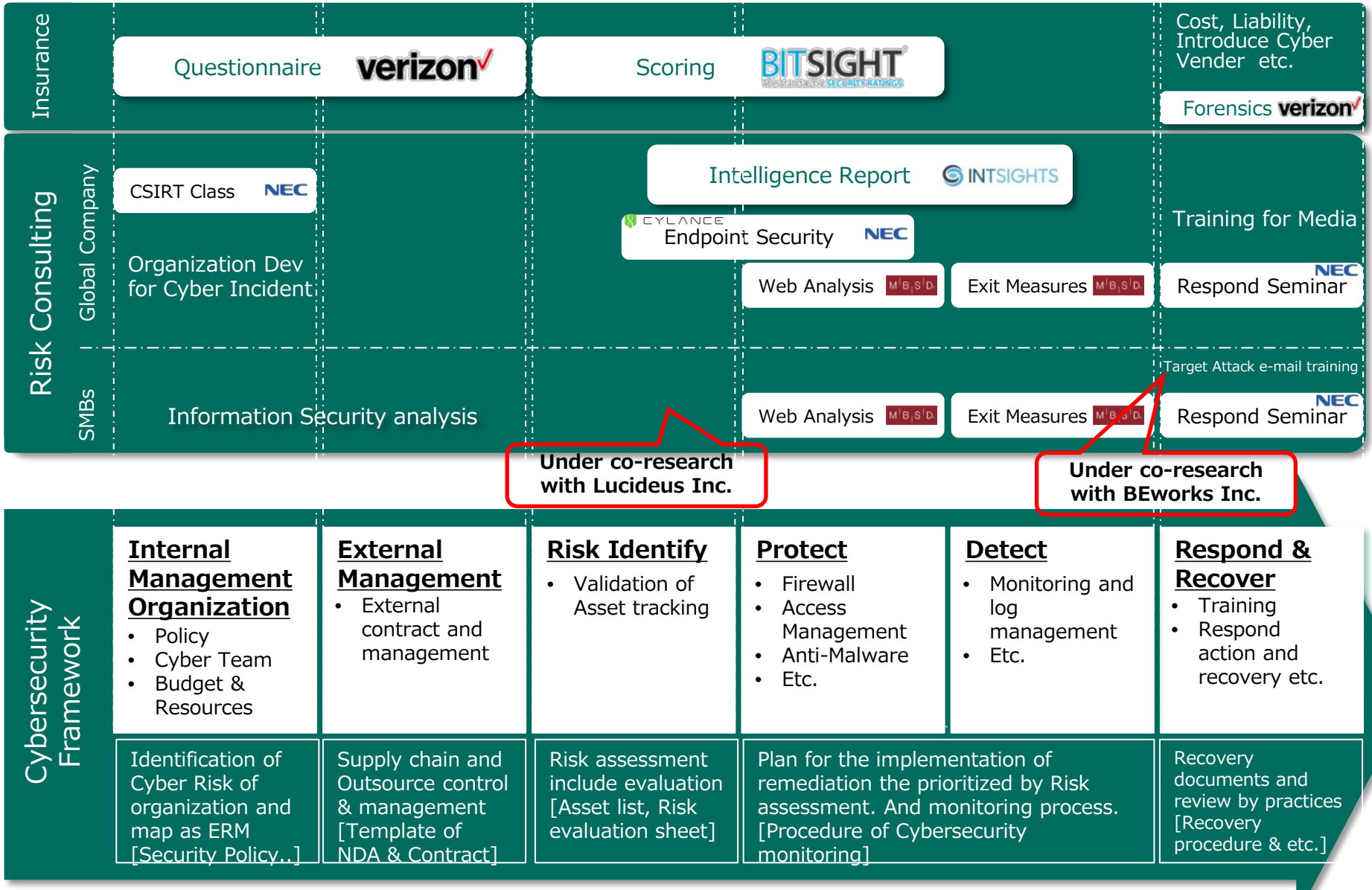
Expectations for additional insurance services(2/2)

"Other" contains "Support for acquisition of certification", "Introduce lawyers who are knowledgeable about security issues", "On-site inspection until recover" and etc..



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,Kanda Awajicho,
Chiyoda-ku, Tokyo 101-0063

Tel : +813-5296-8961／Fax : +813-5296-8940
https://www.irric.co.jp/