



Cyber Index Corporate Survey 2023

December 2023

Japan Federation of IT Organizations
Cyber Security Committee Corporate Assessment Subcommittee

**(1) Importance of Cyber Security
Information Disclosure
(Results of a survey by the Japan
Federation of IT Organizations)**

Trends in cyber risk disclosure (SEC rules)

The U.S. Securities and Exchange Commission (SEC) has adopted new cybersecurity disclosure rules, effective December 15, 2023. Since the rules apply not only to U.S. companies but also to companies outside the U.S. (Foreign Private Issuer, FPI), Japanese companies listed on the SEC must also comply.

Objective.

To enhance and standardize cyber risk management, strategy, governance, and cyber incident disclosures of listed companies, and to improve cyber security standards throughout society

	Contents	Group	Form	Term
Main Requirements	Material Incident Reporting	U.S. securities registered Companies	8-K (Report of important matters)	Within 4 business days of confirming the incident (effective from December 18, 2023)
		Foreign Private Issuer (FPI)	6-K (Report on important matters)	
	Cyber Security Risk Assessment and Management	U.S. securities registered Companies	10-K (Annual report)	Annual report (effective from December 15, 2023)
		Foreign Private Issuer (FPI)	20-F (Annual report)	

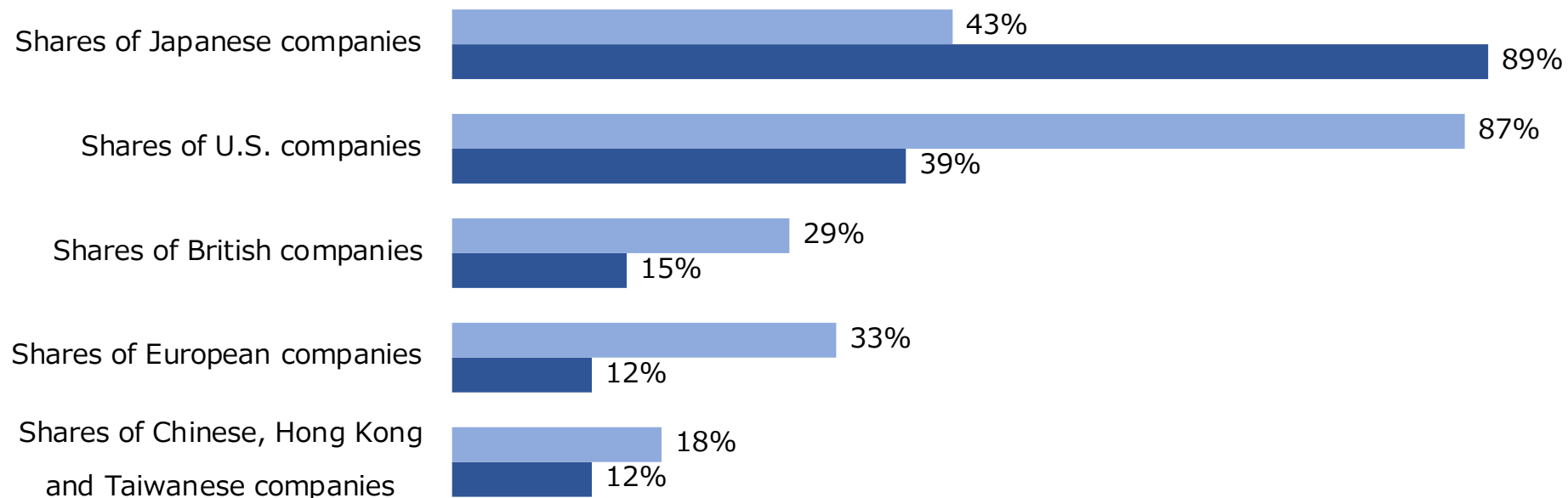
Approximately 40% of the world's market capitalization shares are traded on the New York Stock Exchange and NASDAQ, and approximately 7,000 companies are required to comply with this rule

U.S.-Japan investor cybersecurity awareness survey

In October 2023, the Japan Federation of IT Organizations conducted a survey of 610 Japanese and U.S. investors on their attitudes toward cybersecurity information disclosure.

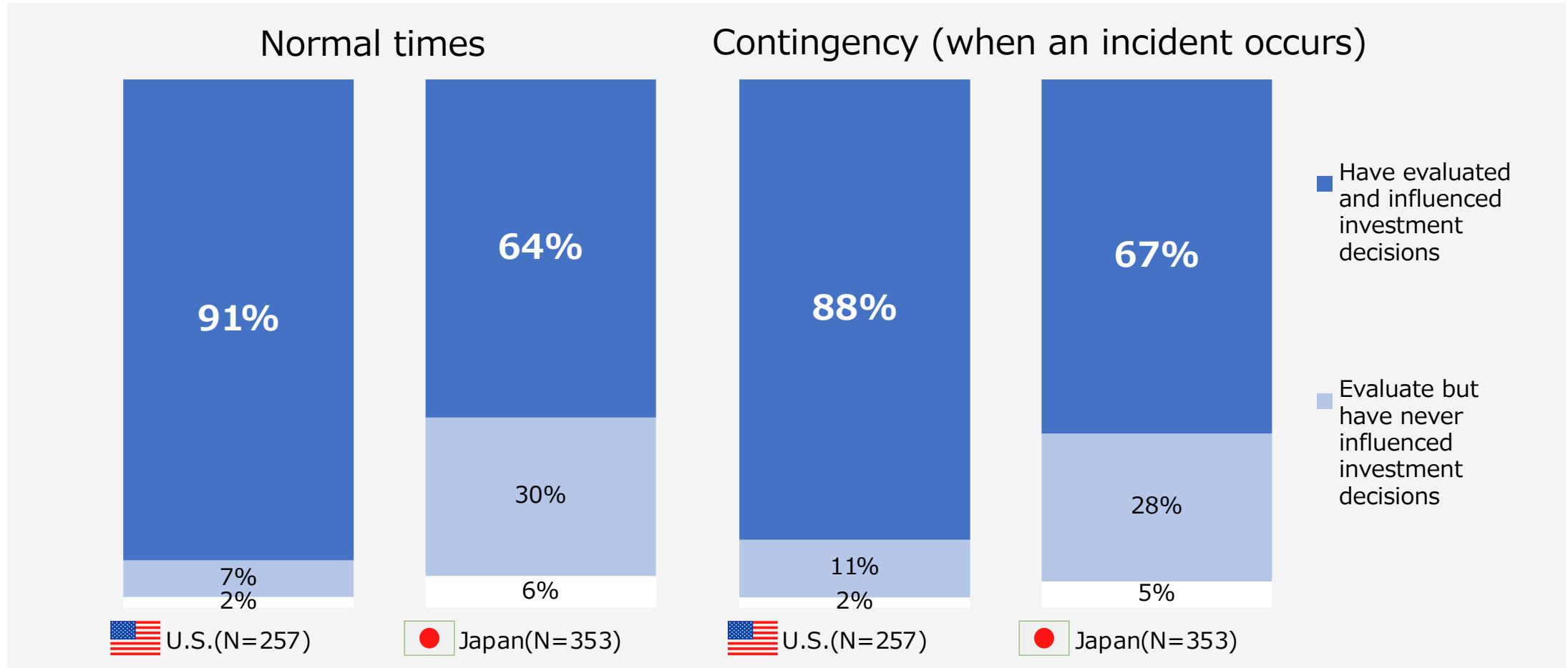
- Survey Objective: To understand institutional investors' awareness and focus on cyber security
- Survey respondents: Japanese and U.S. investors (Japan: 353, U.S.: 257)
- Survey period: September 2023

Attributes of share holdings (N=610)



90% of US investors consider this as part of their investment decisions

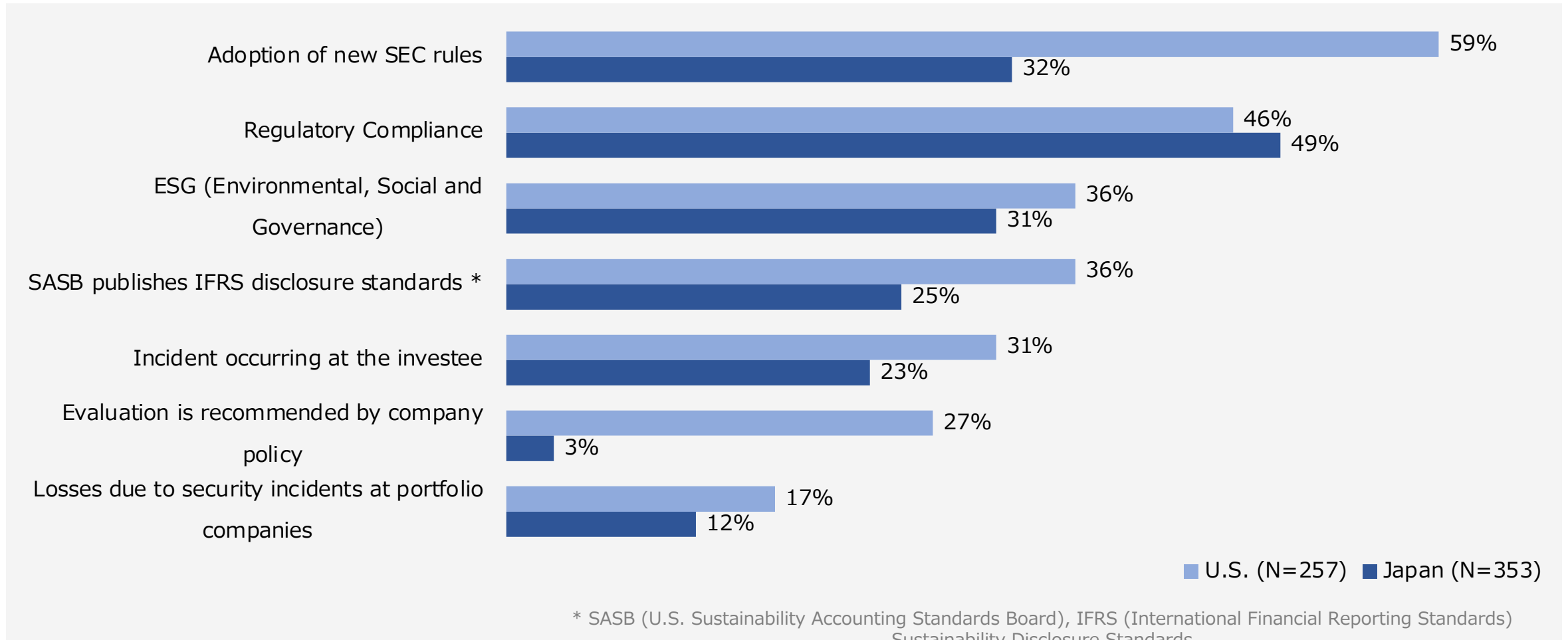
U.S. investors were more than 90% more likely than Japanese investors to have evaluated cybersecurity disclosure as one of their investment decisions and influenced their investment decisions (Japanese investors were 60%, or 27.4 percentage points lower)



Percentage of respondents who evaluated cybersecurity-related disclosure (normal times and contingency) and its influence on their investment decisions.

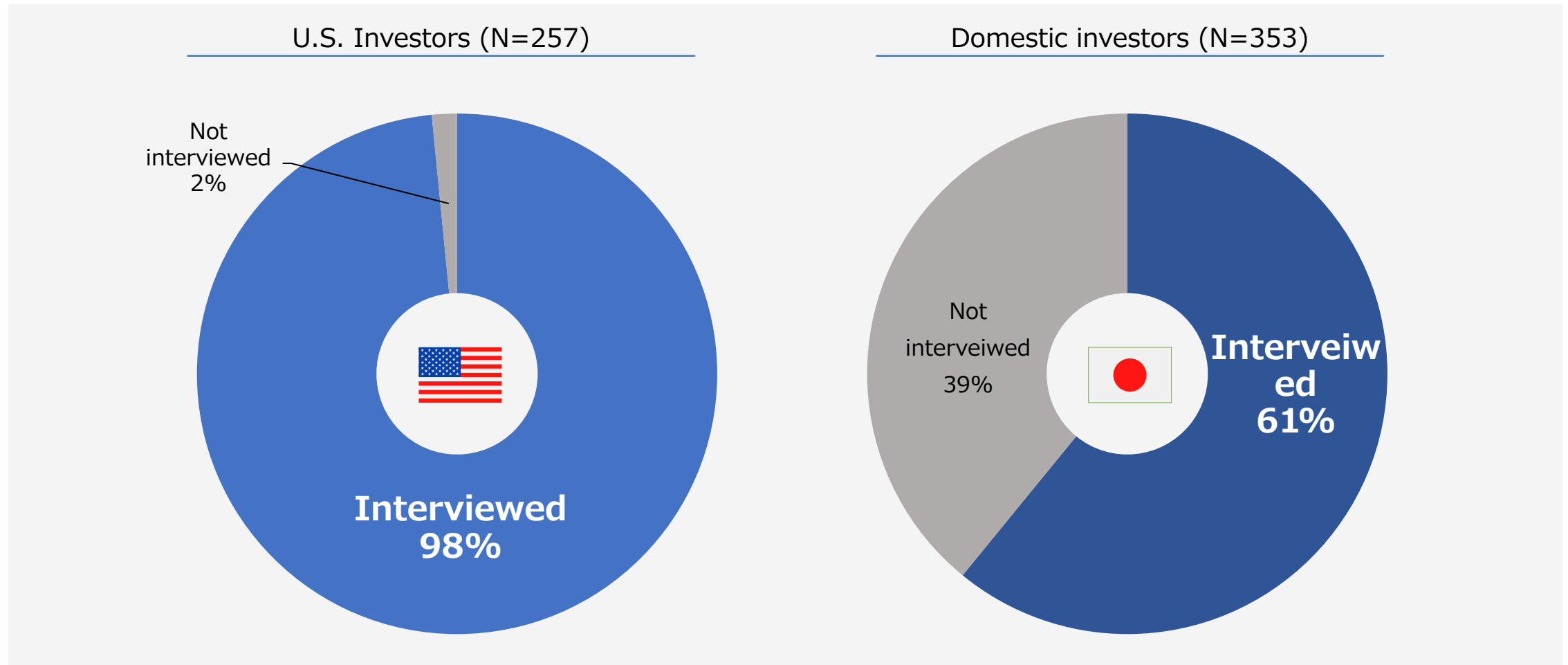
Tighter regulations raise investors' cybersecurity awareness

The top reason for placing importance on disclosure is 'SEC cybersecurity disclosure mandates' at 60% for U.S. investors, and legal regulations at 50% for Japanese investors



Percentage of cybersecurity interviews with portfolio companies

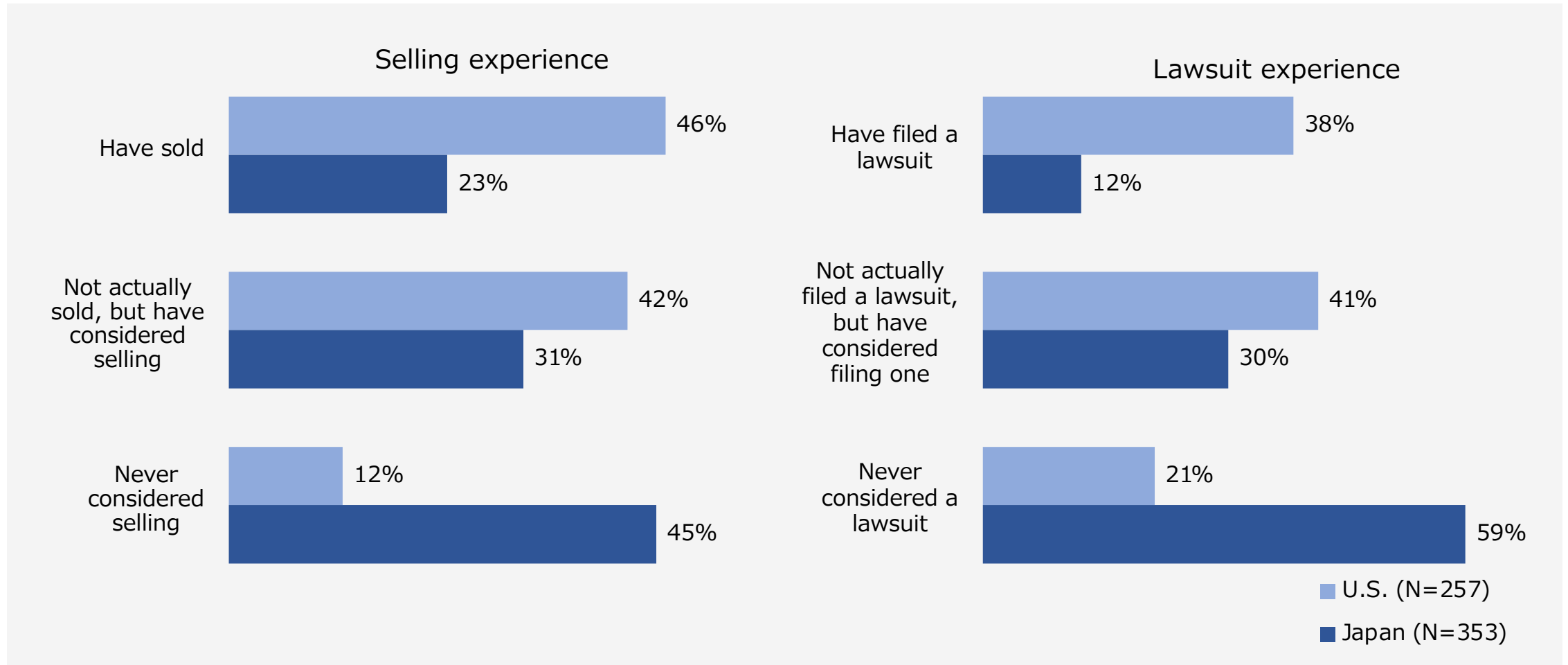
U.S. investment institutions are 98% more likely than Japanese investors to interview their portfolio companies about cybersecurity (61% in Japan)



Percentage of interviews about cybersecurity in dialogue with portfolio companies

40% of U.S. investors have experienced an incident-related sale or lawsuit

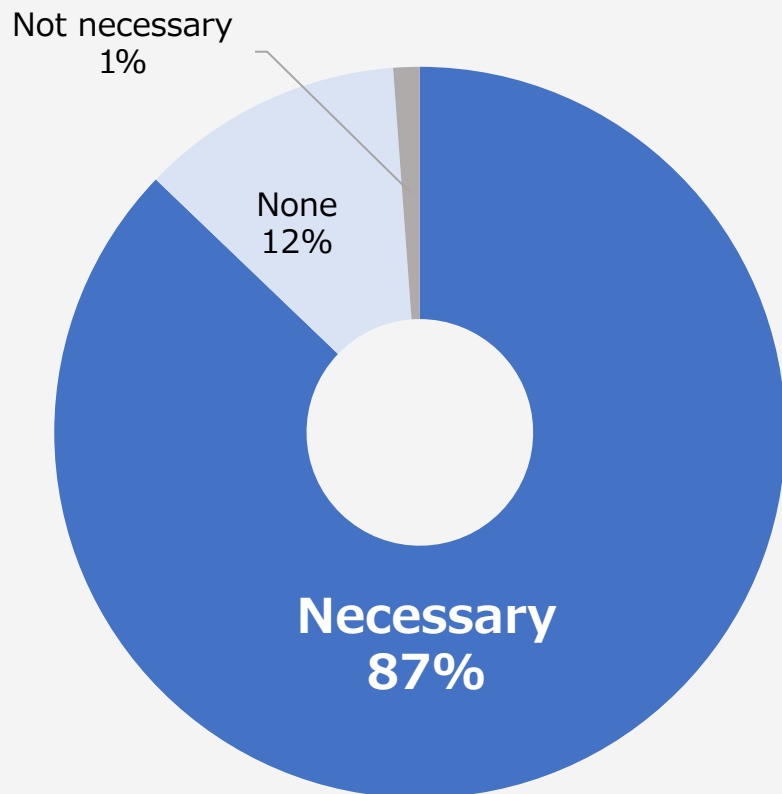
U.S. investors are more likely than Japanese investors to have sold their portfolio companies due to cyber incidents (46% in the U.S., 23% in Japan)



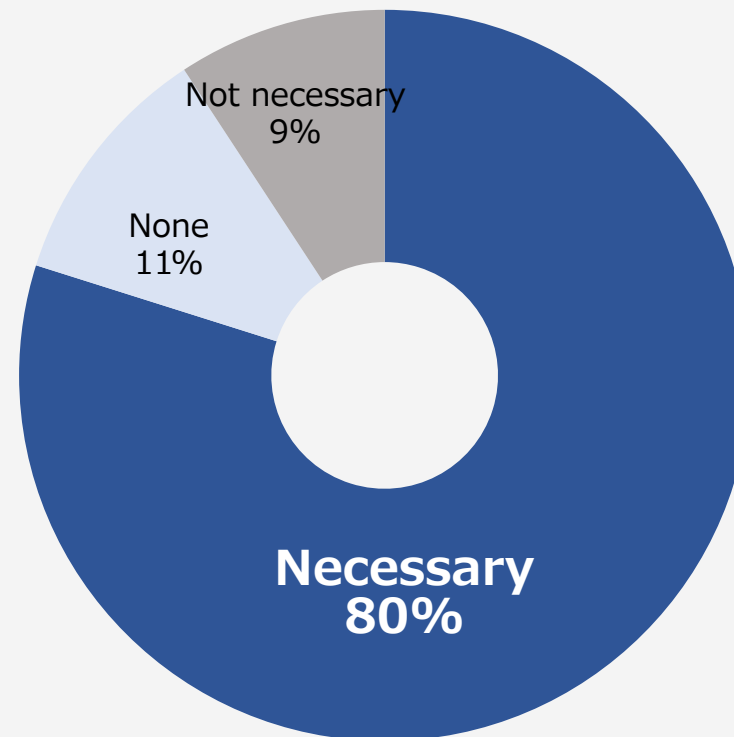
The Need for Cybersecurity Indicators

More than 80% of Japanese and U.S. investors answered that they need a cybersecurity-specific index provided by a third-party organization, and they are looking for a security index that simplifies making investment decisions.

U.S. Investors (N=257)



Domestic investors (N=353)



Need for third-party cybersecurity-specific indicators

Results of individual interviews with investors



Domestic
Institutional
Investors

If lack of organizational governance, including cybersecurity, is confirmed, it may be reflected in the resolution of confidence of directors as a comprehensive decision by shareholders

Management (such as CIO,CISO) must be able to answer questions directly without a script from foreign investors after a major incident at their company



Foreign
company
rating agency



Domestic
Institutional
Investors

Standards for disclosure of cybersecurity information are necessary. It is difficult to make investment decisions unless comparable information is available.

(2) Cyber Index Corporate Survey 2023

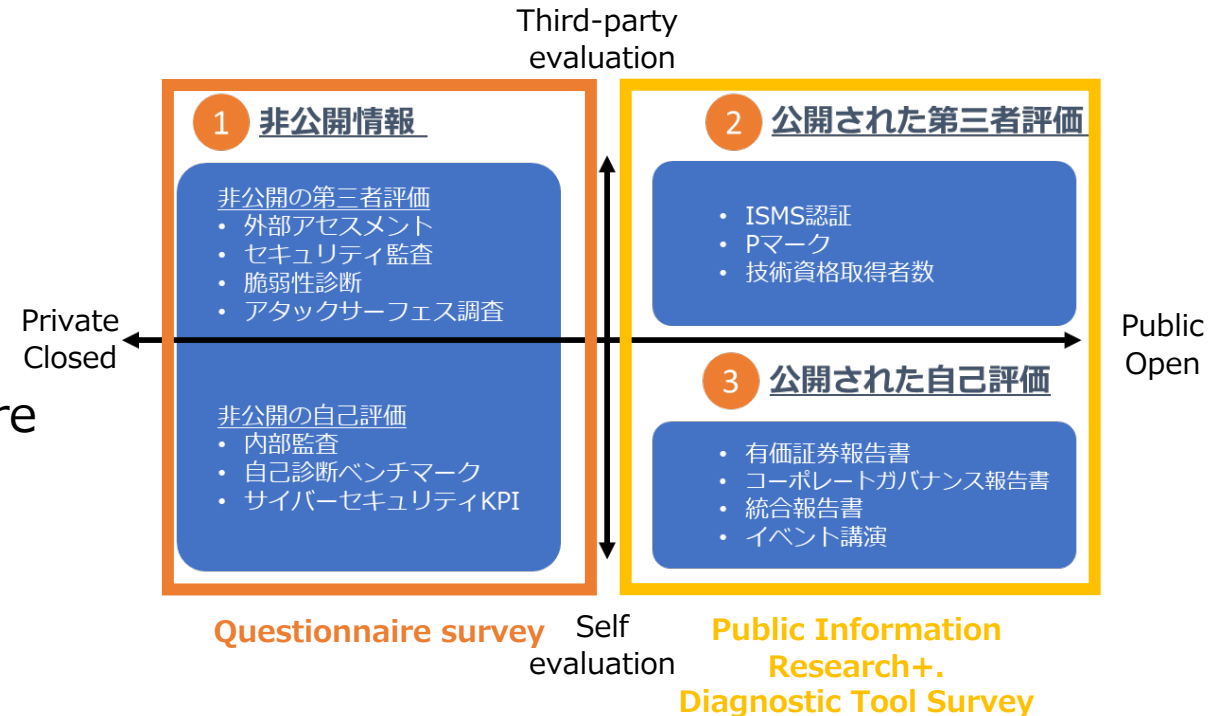
What is the Cyber Index Corporate Survey?

With the aim of **promoting the disclosure of information on** cybersecurity measures taken by private-sector companies, a survey on cybersecurity initiatives was conducted among the companies that comprised the Nikkei 500.

Companies that demonstrated excellent cyber security measures and information disclosure were given a star rating and commended.

Company Survey Details

- Conducted a comprehensive survey on corporate cybersecurity initiatives and disclosure stance by conducting a questionnaire survey and public information survey.
- Continuing from last year, the results of diagnostic tool surveys of attack surfaces were also added to the evaluation.
- ‘Ratings’ based on original survey items developed by the Corporate Evaluation Subcommittee



Items	FY2020	FY2021	FY2022	FY2023
Target Company	Nikkei 225 Component Index	Nikkei 500 Component Index	Nikkei 500 Component Index	Nikkei 500 Component Index
Public Information	Applicable	Applicable	Applicable	Applicable
Non-public information	Not applicable	Applicable	Applicable	Applicable
Diagnostic Tool Survey	Not applicable	Not applicable	Applicable	Applicable

Survey methodology for the Cyber Index Corporate Survey 2023

- Target: 500 companies that comprise the Nikkei 500 Index
- Period: July - September 2023
- Overall score: Sum of the following 3 items
- Survey Description:

Public Information

Surveyed securities reports, corporate governance reports, integrated reports, and corporate website entries, as well as event speeches, ISMS certifications, P-marks, and number of technical certifications obtained.



Annual Securities Reports, etc.

Survey

Conducted a survey of companies to ascertain their cybersecurity initiatives that are not publicly disclosed, and created original questions based on the IPA Cybersecurity Visualization Tool.



Questionnaire survey
(Total 21 questions)

Diagnostic Tool Survey

To investigate the degree of risk of the attacked area from an external perspective, the scores from the Attack Surface diagnostic tool survey conducted by the U.S. Security Scorecard (SSC) are used.





Attack surface
Survey of tools to

Cyber Index Corporate Survey 2023 Results

Two stars were awarded to the 14 companies that demonstrated particularly outstanding efforts and information disclosure on an ongoing basis.

Cyberindex Corporate Assessment 2023 Results

Rating	Evaluation basis	Number of companies
	Companies that have demonstrated a <u>particularly outstanding commitment and information disclosure on an ongoing basis</u>	14 11 companies last year
	Companies with <u>excellent initiatives and information disclosure</u>	44 35 companies last year