2024 Cybersecurity Benchmarking Survey

Report of Findings

NSCP
NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

ACA Aponix®

“The Cybersecurity Benchmarking Survey continues to be a valuable resource to compliance professionals seeking insight about current and emerging cybersecurity trends, policies, and challenges across the financial services industry. We are particularly proud of our partnership with ACA Group to help firms prioritize their cybersecurity programs.”

Lisa Crossley, Executive Director, NSCP

"Our survey findings underscore the critical importance of staying ahead of evolving cybersecurity threats. As nearly half of the respondents express uncertainty about SEC enforcement, it's clear that regulatory compliance remains a top concern.”

Mike Pappacena, Partner, ACA Aponix

The *2024 Cybersecurity Benchmarking Survey*, a joint project of ACA Group and the National Society of Compliance Professionals (NSCP) fielded online between January and February, covered a wide range of topics. ACA Aponix®, part of ACA Group, and the NSCP conduct the survey biannually to help firms better manage increasing expectations and uncertainty around cybersecurity risk.

Compliance professionals at 308 investment adviser firms participated in the survey. All firm sizes were represented and responding firms belonged to varied business types, with most responses coming from asset managers/non alternatives, broker-dealers, and alternative investment advisers.

The 2024 Cybersecurity Benchmarking Survey yielded notable findings in several areas of interest, including regulatory preparedness, AI risk management, cybersecurity threats and cybersecurity preparedness, as well as cyber insurance and vendor cybersecurity.

NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

Table of Contents

NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

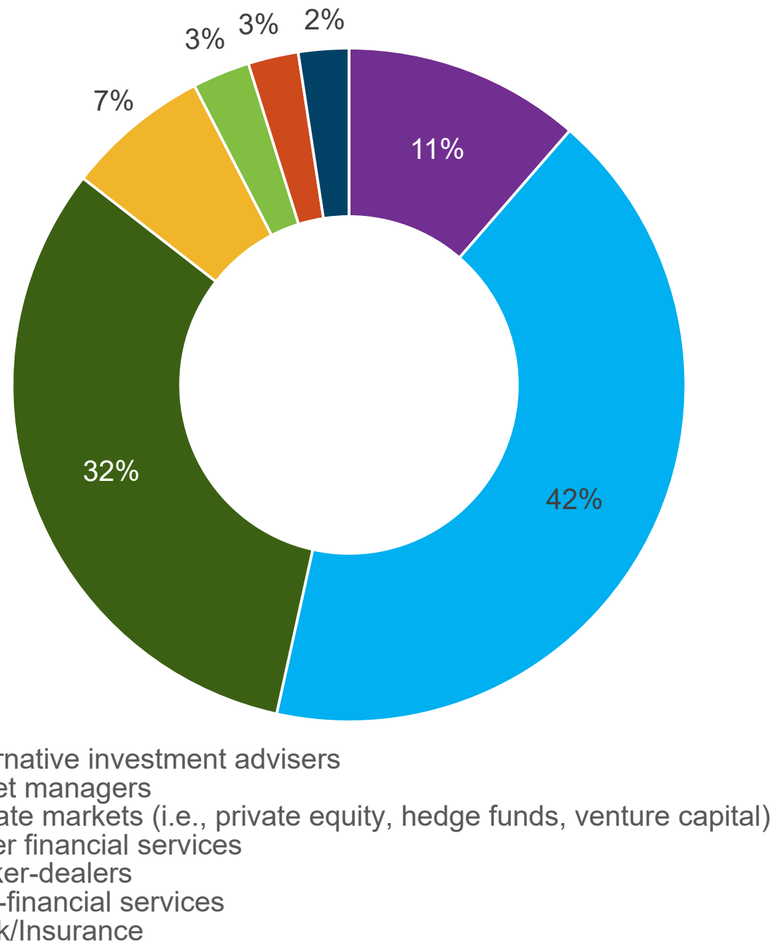
Demographics

Multiple Business Types Represented

What would you best classify your business as?

Analysis:

- 308 Responses collected between January and February 2024.
- Survey shared through email and social media channels by the NSCP and ACA Group.
- Respondents belonged to varied business types, with most responses coming from asset managers/non-alternatives investment advisers and private markets.

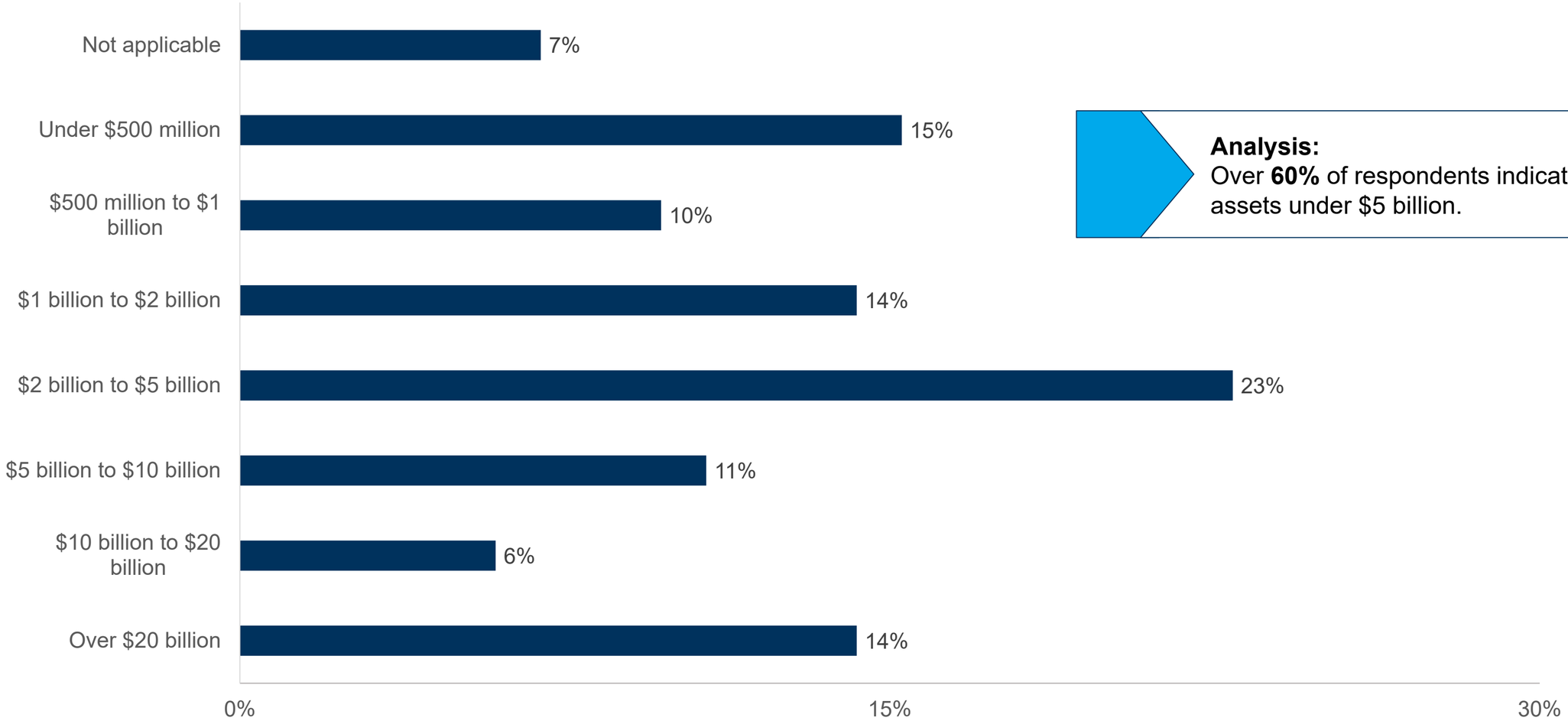


N = 288

NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

Respondents Represented Firms With Varied Asset Values

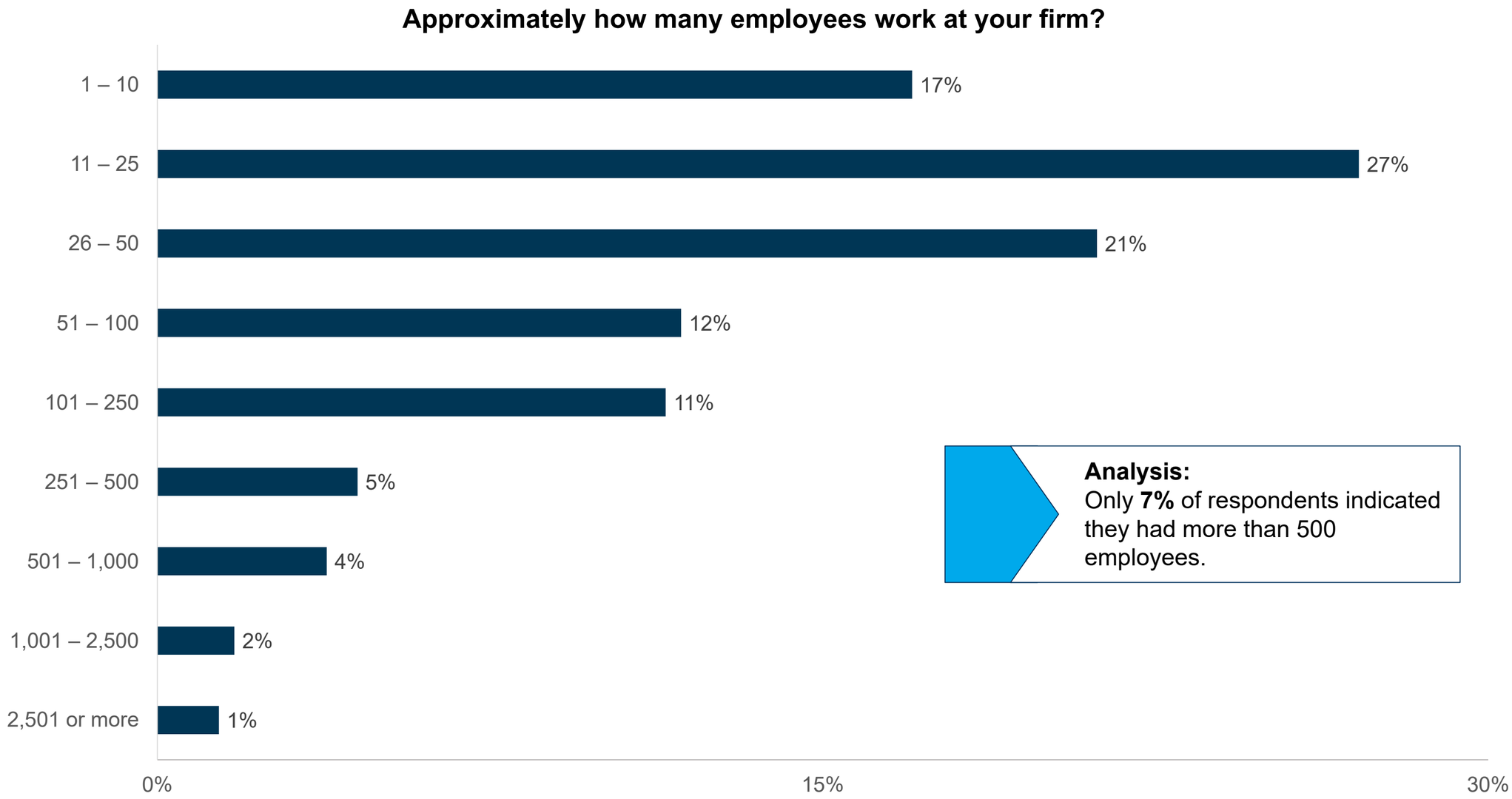
What is your firm's total regulatory assets under management?



Analysis:
Over **60%** of respondents indicated assets under $5 billion.

N=288

Respondents Represented Primarily Small Firms



Analysis:
Only **7%** of respondents indicated they had more than 500 employees.

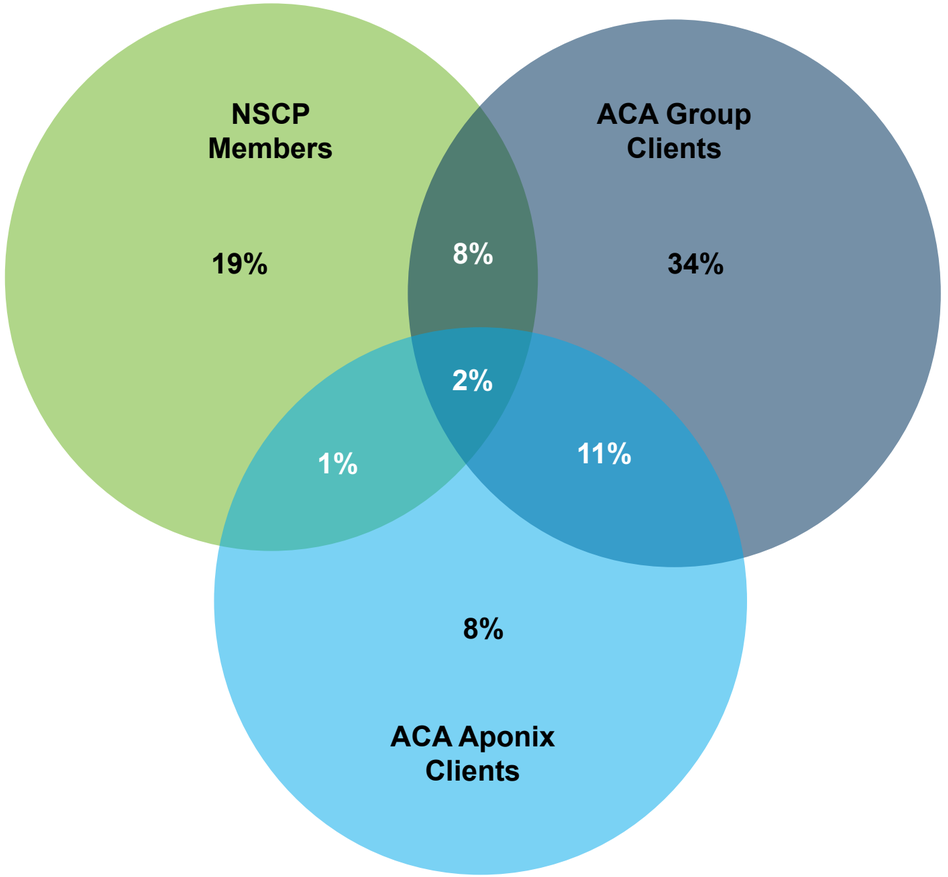
N=288

Distribution Channels Were Effective

My firm's relationship to ACA Group and/or NSCP is: (Select all that apply)

Analysis:

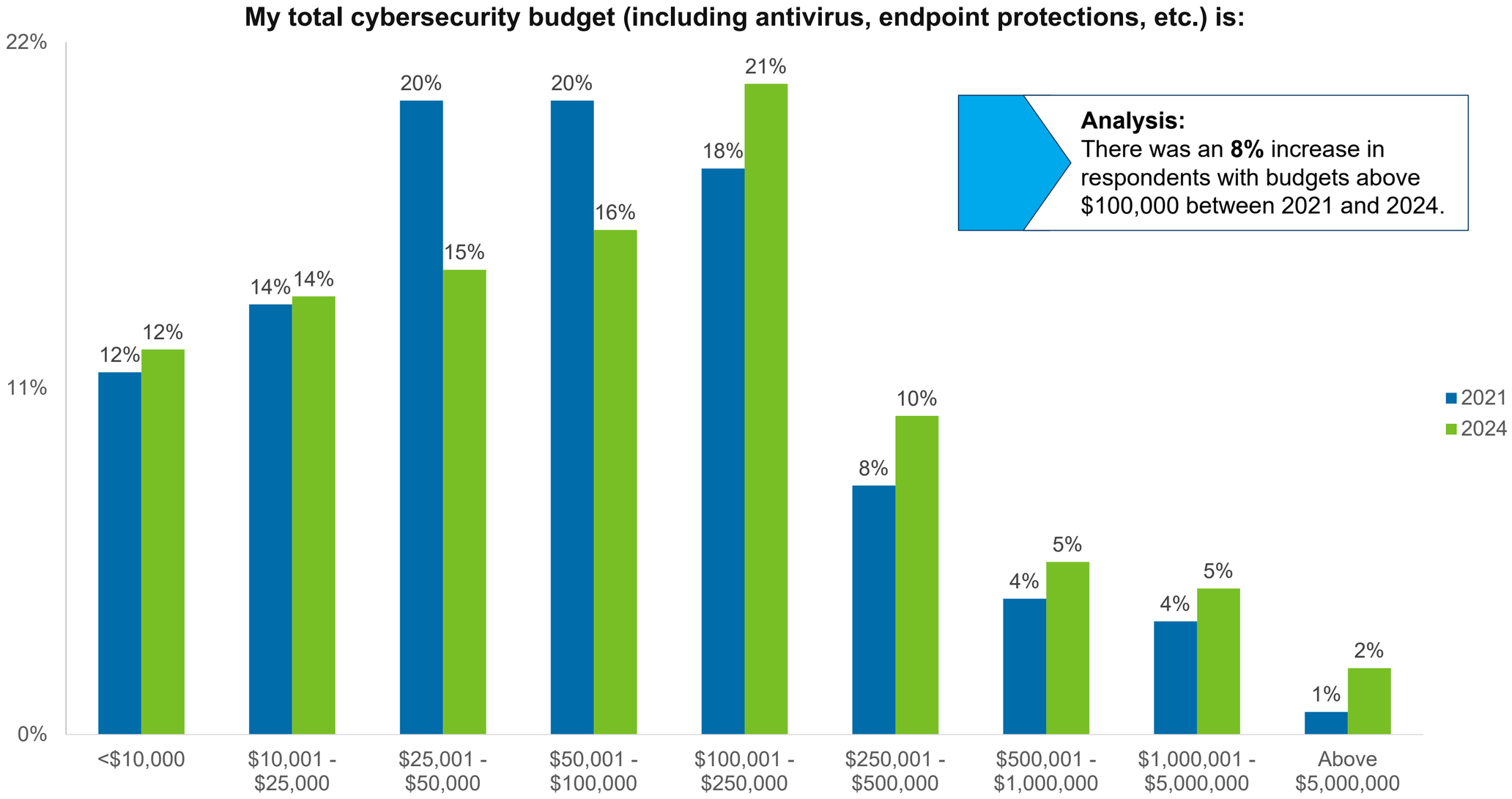
- Most respondents identified as clients of ACA Group, with **55%** of respondents indicating they were clients..
- Social media distribution of the survey allowed for the participation of multiple respondents with no association to ACA or the NSCP, with nearly **15%** of respondents indicating no relationship to either organization.



N=288

Cybersecurity Budget and Staffing

Cybersecurity Budgets Are Increasing

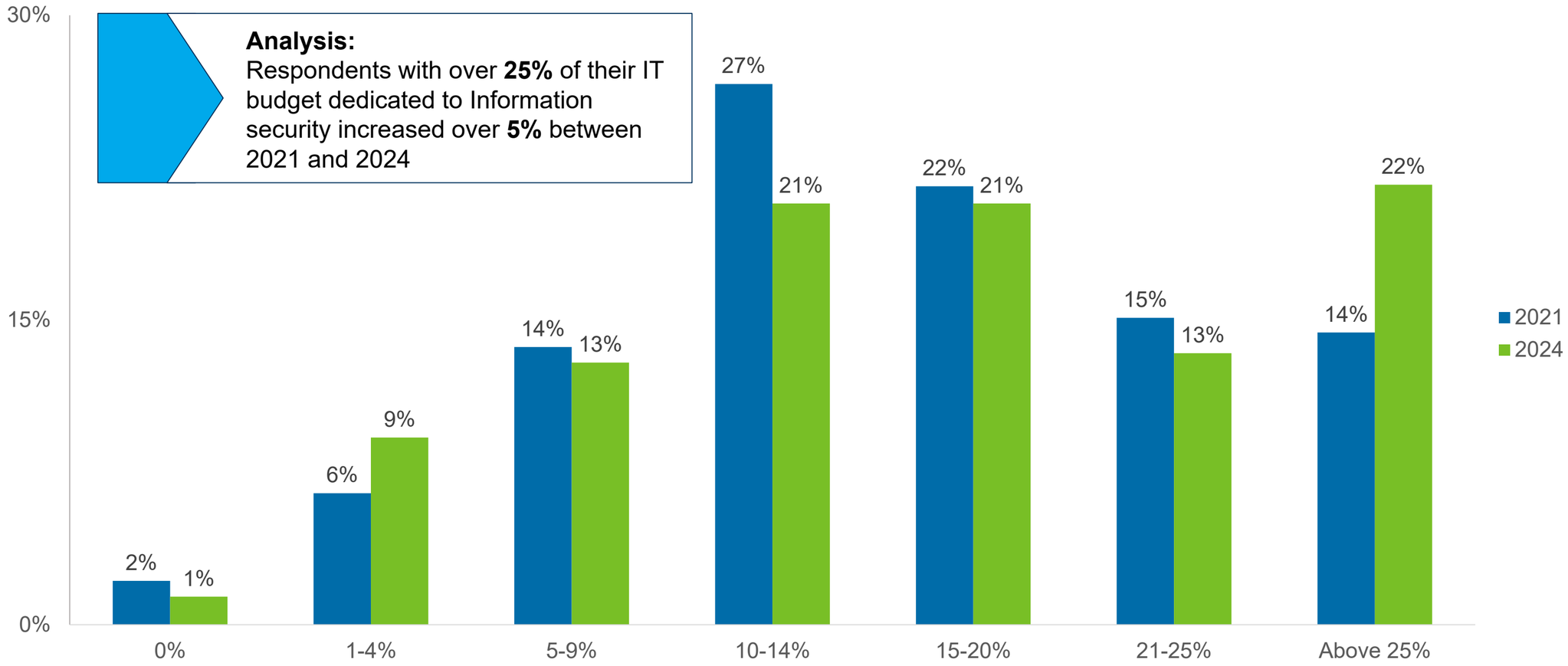


NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

2021 N = 139
2024 N = 237

IT Budgets Increasingly Dedicated to Information Security

As a percentage of the total IT budget (information security spend divided by total IT spend), information security is approximately:



2021 N = 139
2024 N = 217

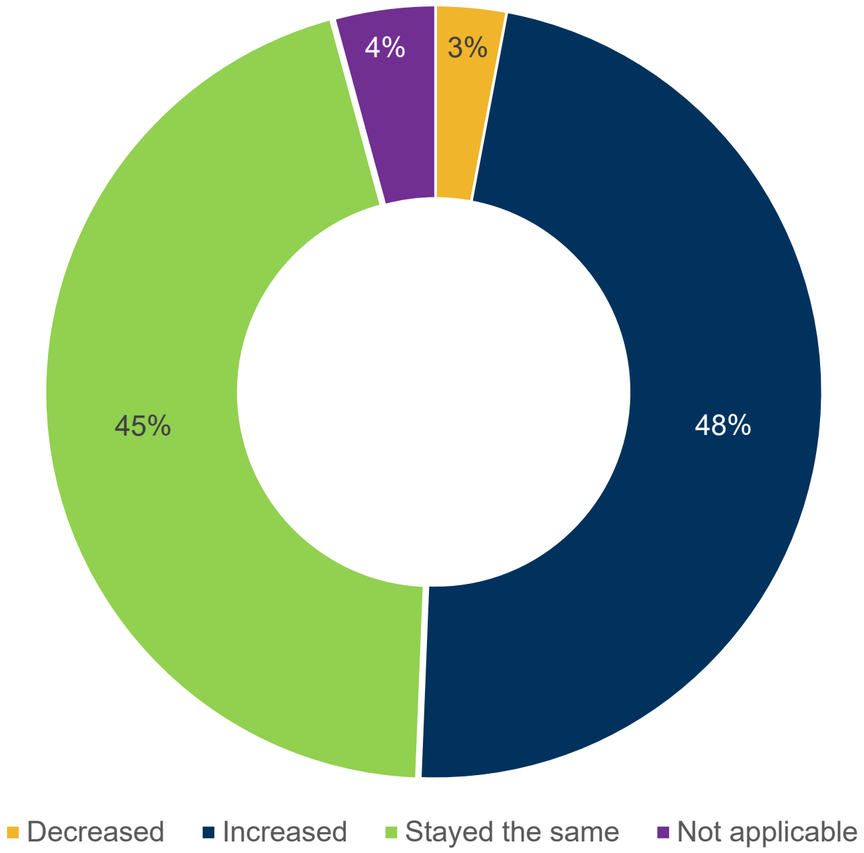
* 2024 Data excludes respondents who selected “Not Applicable” to this question. The option was not available in the 2021 version of the survey.

Cybersecurity Budgets Increase Year Over Year

How has your program's 2024 cybersecurity budget changed when compared to your program's 2023 cybersecurity budget?

Analysis:

- Approximately **48%** of respondents indicated their cybersecurity budgets increased between 2023 and 2024.
- The median reported increase was **11%**.
- Only **3%** of respondents indicated a decrease in budget between 2023 and 2024.

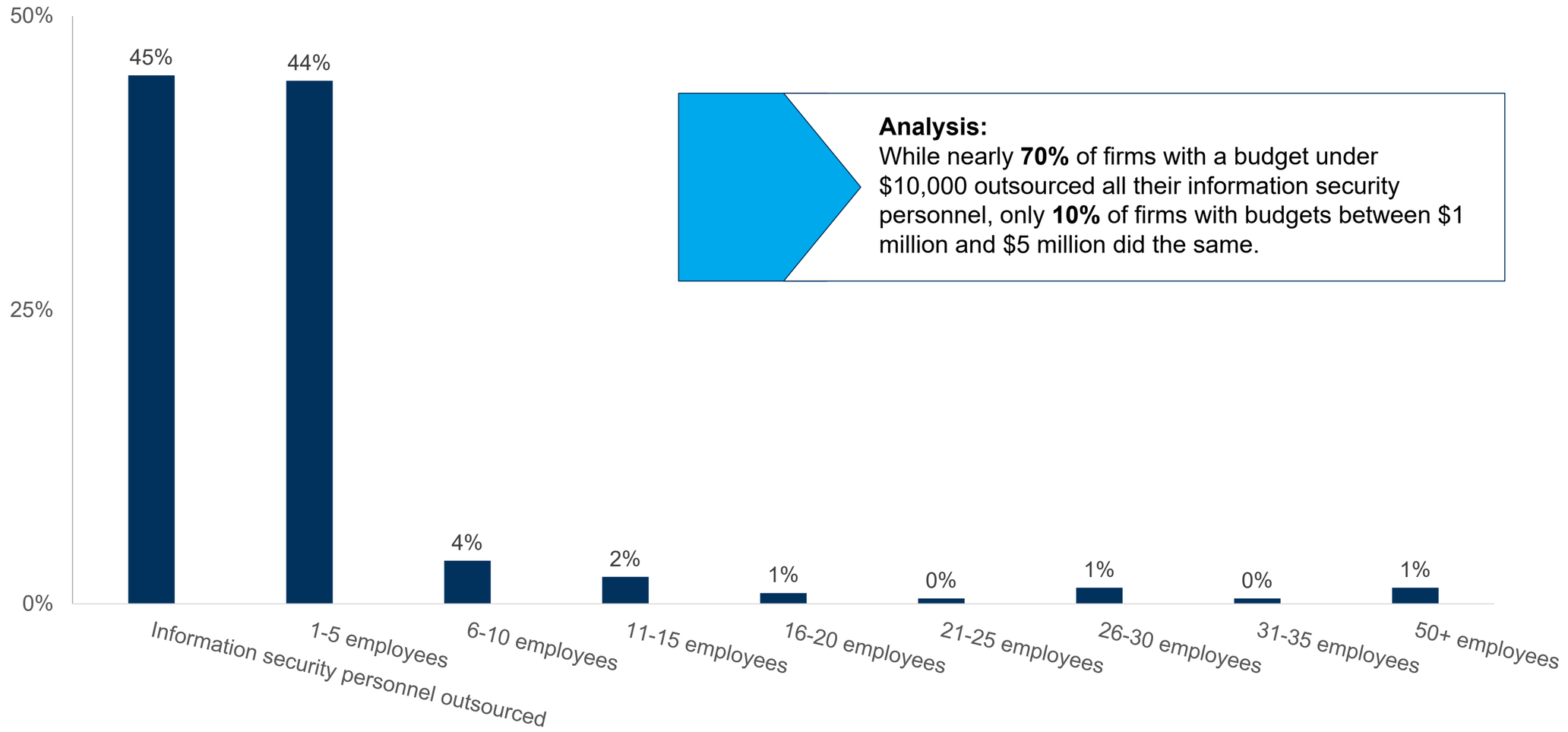


NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

N = 237

Information Security Teams are Small or Outsourced

How many full-time information security employees do you currently have working within your firm?



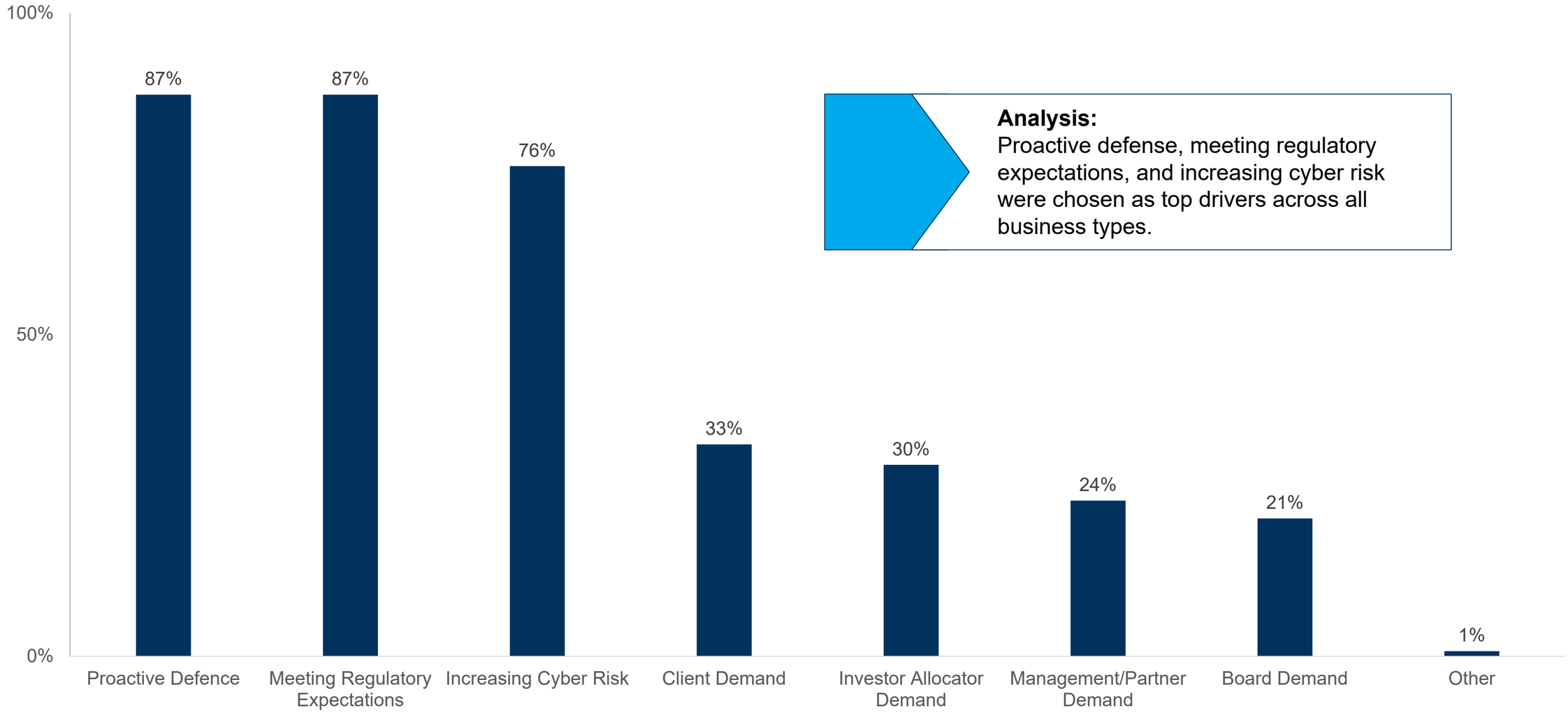
Analysis:
While nearly **70%** of firms with a budget under $10,000 outsourced all their information security personnel, only **10%** of firms with budgets between $1 million and $5 million did the same.

N = 218

Cybersecurity Concerns

Cybersecurity at Most Firms Driven by Same Reasons

What are the primary drivers for your focus on cyber security in your organization? (Select all that apply)

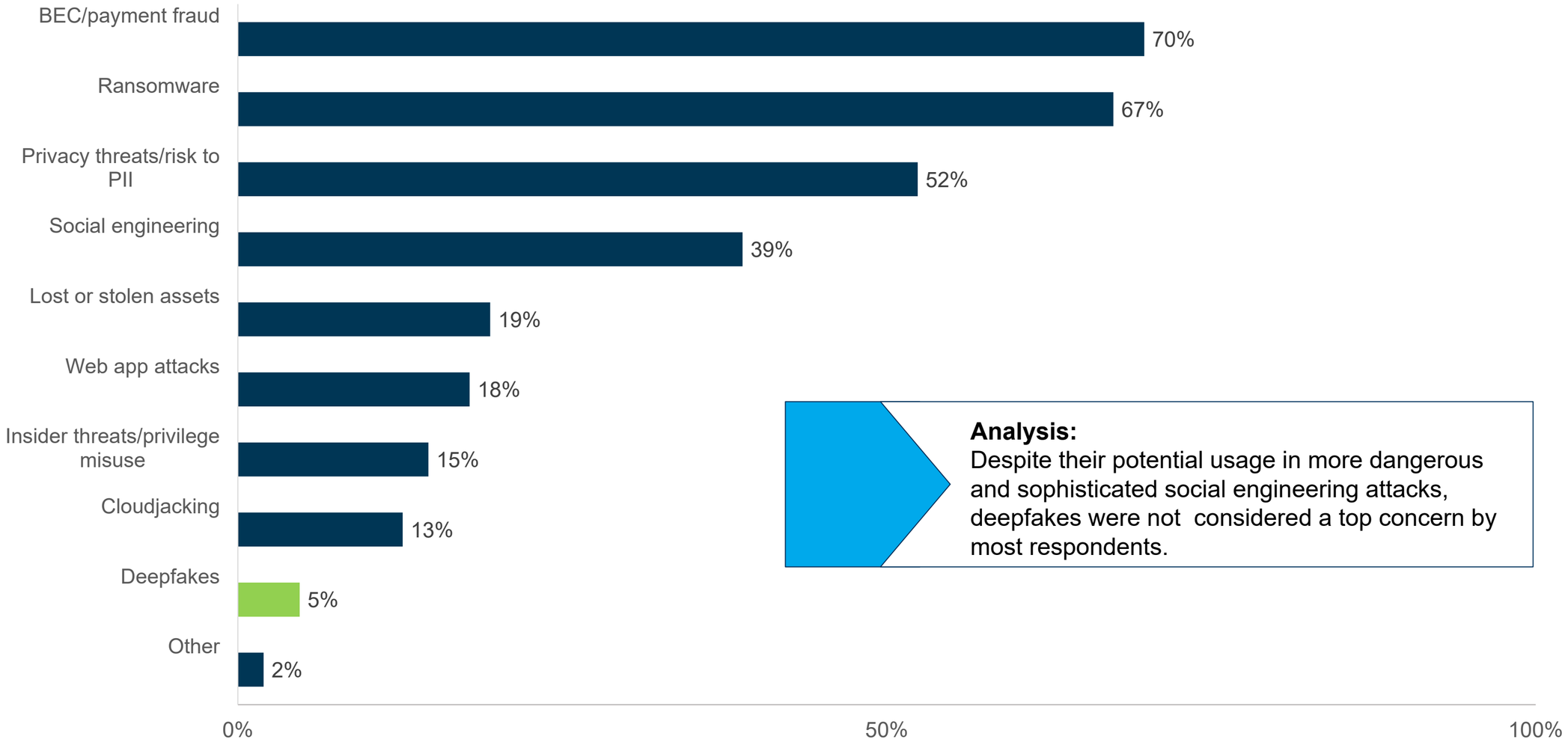


Analysis:
Proactive defense, meeting regulatory expectations, and increasing cyber risk were chosen as top drivers across all business types.

N = 252

Some Cybersecurity Threats May Be Overlooked

Which of the following cybersecurity threats is your firm most concerned about? (Please select the top three)



Analysis:
Despite their potential usage in more dangerous and sophisticated social engineering attacks, deepfakes were not considered a top concern by most respondents.

N = 252

Cybersecurity Preparedness

Data Centers and Regulatory Mock Exams Often Overlooked

How often do you conduct the following?

Policy and Infrastructure Assessment and Review								
	Weekly	**Monthly**	**Quarterly**	**Semi-annually**	**Annually**	**Every other year**	**Ad-hoc**	**Never**
Review of cybersecurity policies and procedures	0.00%	1.84%	6.91%	8.76%	74.19%	1.84%	4.61%	1.84%
Regulatory mock exam	0.00%	0.92%	1.84%	3.23%	26.27%	7.83%	34.10%	25.81%
Cybersecurity program maturity assessment	0.92%	3.23%	10.14%	4.61%	48.85%	3.23%	14.75%	14.29%
Cybersecurity risk assessment	2.30%	4.15%	11.98%	4.15%	63.13%	3.23%	9.22%	1.84%
Data center on-site visits	3.23%	1.84%	2.76%	4.15%	13.36%	2.30%	21.66%	50.69%

* Highlighted cells indicate most selected performance frequency for each test or assessment

NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

N = 217

Phishing Tests Are More Frequently Implemented Than Other Response Tests

How often do you conduct the following?

System and Response Testing								
	Weekly	**Monthly**	**Quarterly**	**Semi-annually**	**Annually**	**Every other year**	**Ad-hoc**	**Never**
Table-top incident response exercise	0.00%	1.84%	3.23%	6.91%	39.63%	5.07%	17.51%	25.81%
Phishing testing	7.83%	36.87%	30.88%	6.45%	5.53%	0.92%	7.37%	4.15%
Network penetration testing	2.76%	5.07%	8.29%	6.91%	52.07%	7.83%	8.29%	8.76%
Internal vulnerability assessment	12.90%	16.13%	13.82%	3.69%	32.26%	4.61%	10.60%	5.99%
External network vulnerability assessment	15.21%	11.52%	9.22%	4.15%	41.47%	5.07%	7.83%	5.53%
Application security assessment	9.68%	8.76%	13.82%	7.83%	31.80%	0.92%	20.74%	6.45%

* Highlighted cells indicate most selected performance frequency for each test or assessment

NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

N = 217

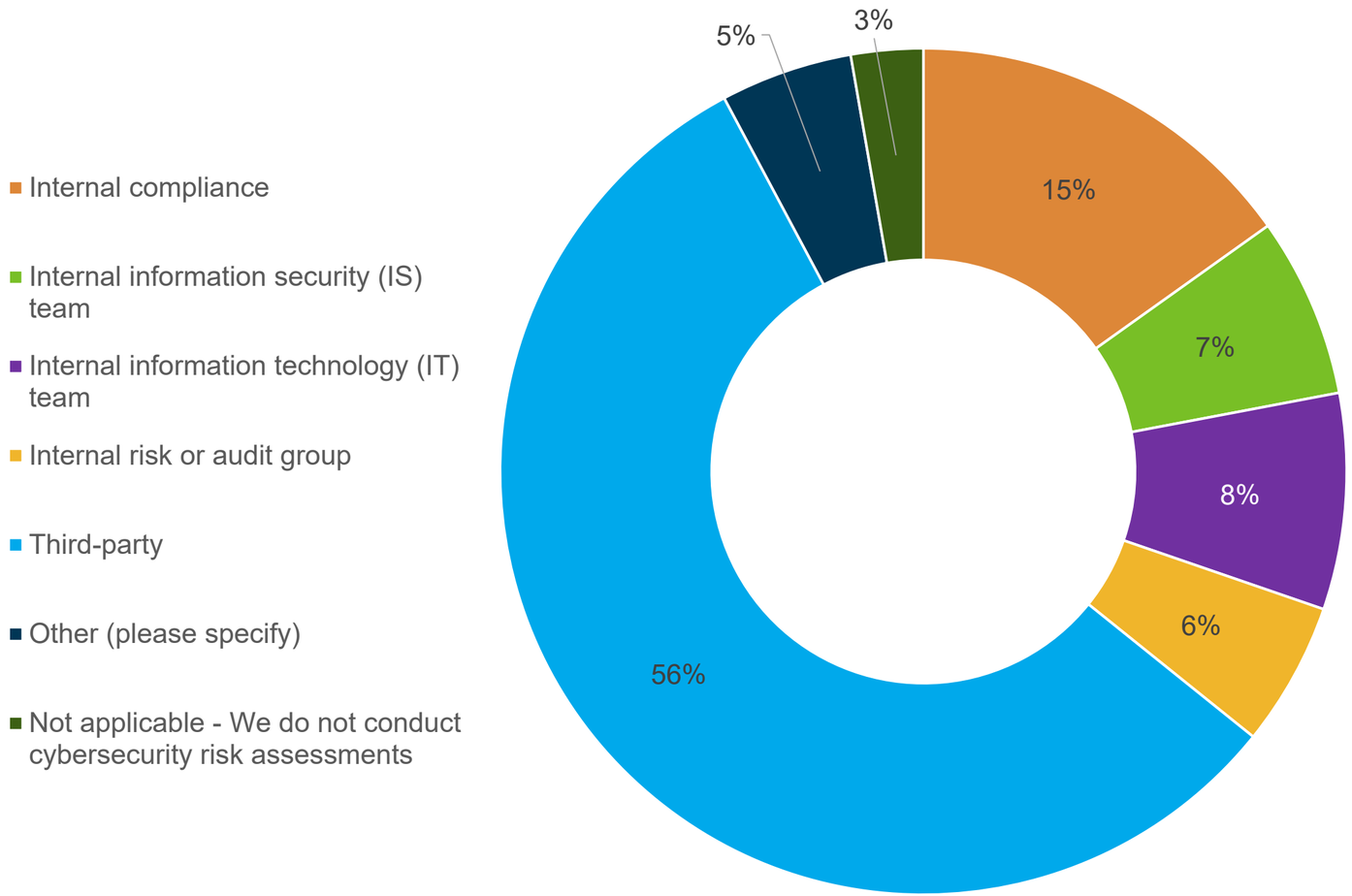
Third-Party Providers Are Key In Assessing Risk

Do you conduct cybersecurity risk assessments using internal resources or a third-party?

Analysis:

Over **50%** of firms rely on third-party providers to conduct cybersecurity risk assessments.

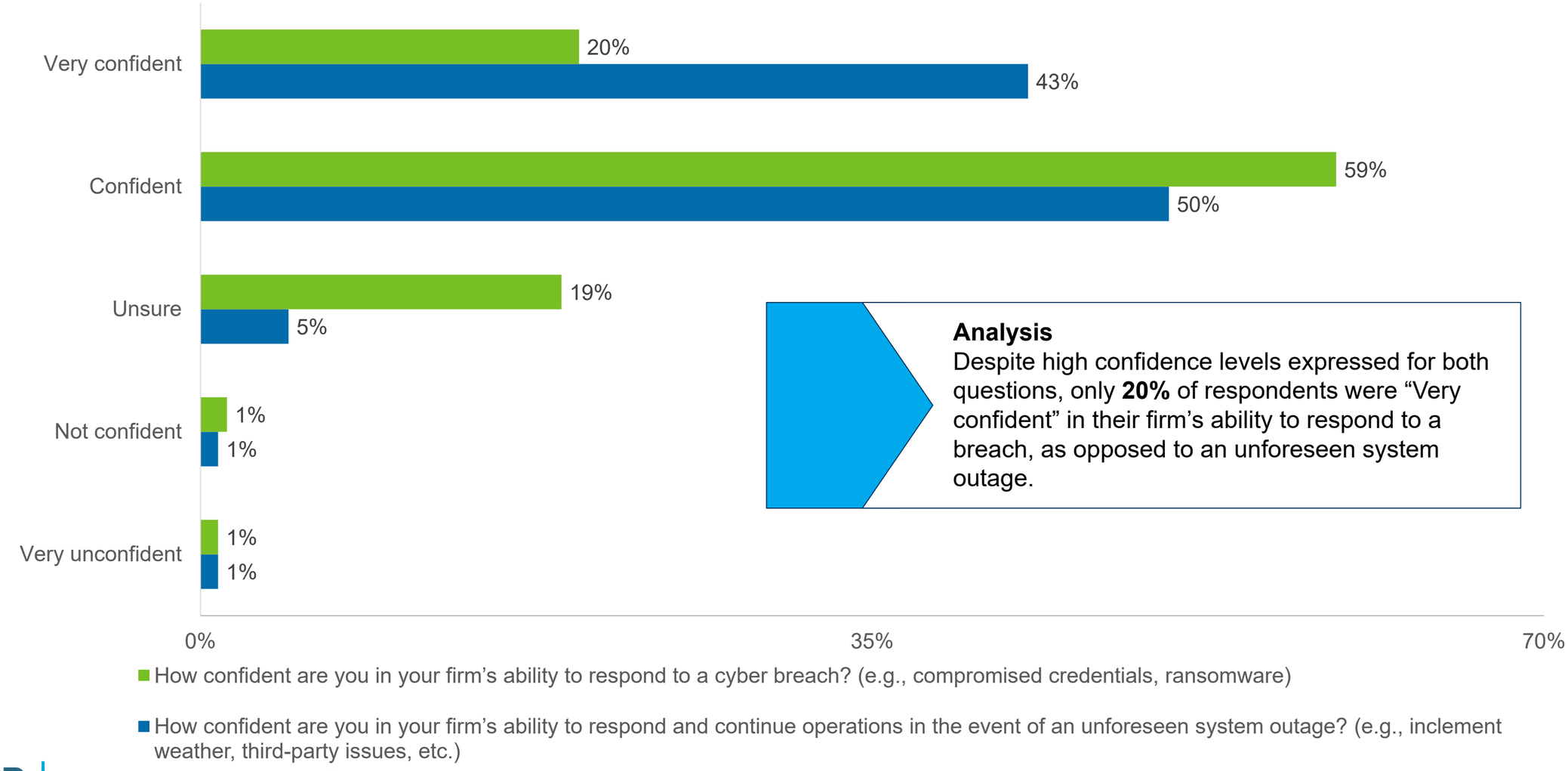
Only about **5%** of firms use an internal risk or audit group.



N = 218

Firms Are Generally Confident in Ability to Respond to Incidents

Firm confidence in responding to a cybersecurity breach vs. firm confidence in responding to unforeseen system outage



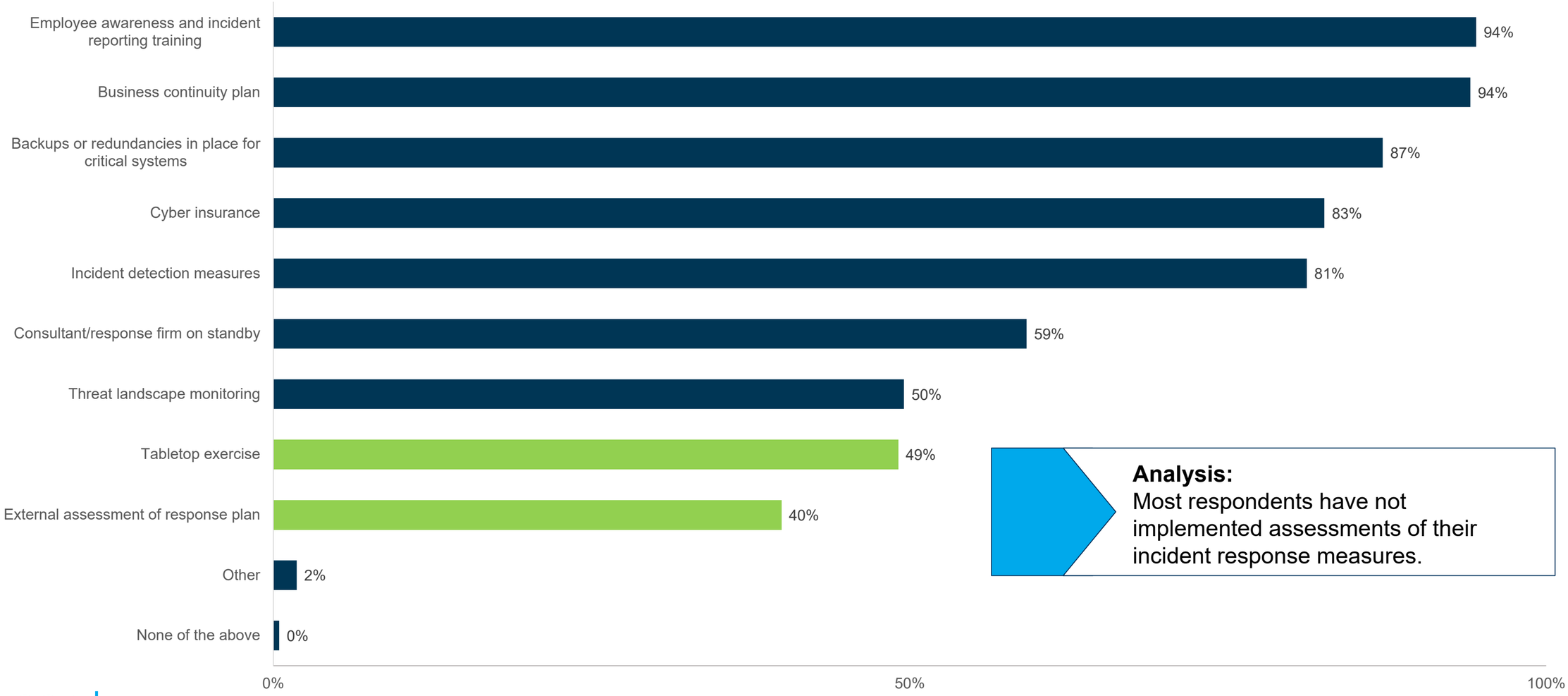
Analysis
Despite high confidence levels expressed for both questions, only **20%** of respondents were "Very confident" in their firm's ability to respond to a breach, as opposed to an unforeseen system outage.

NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

N = 218

Incident Response Measures Are Often Untested

Which of the following items has your firm implemented to prepare the company to respond to a cyber incident (e.g., compromised credentials, ransomware, etc.)? (Select all that apply)

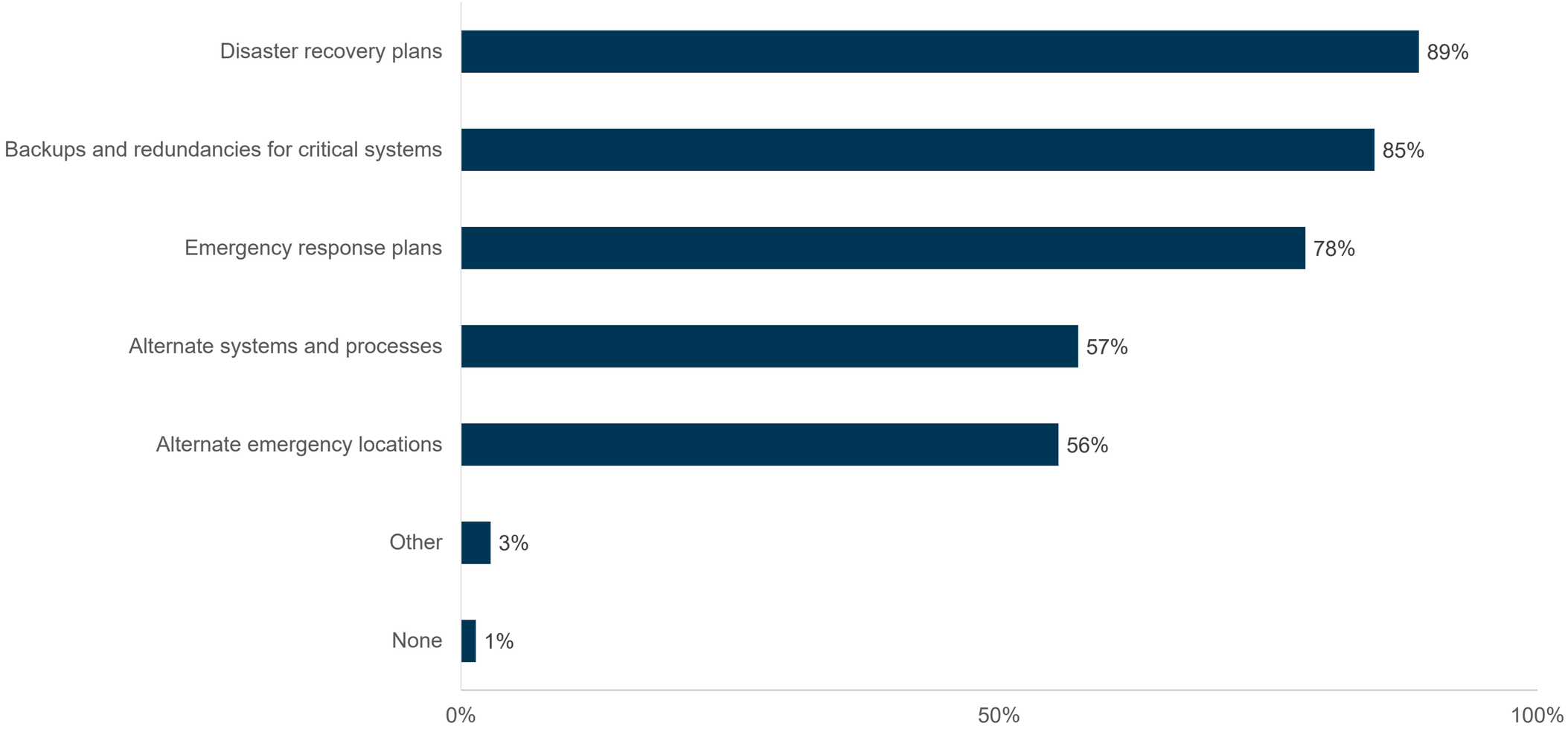


Analysis:
Most respondents have not implemented assessments of their incident response measures.

N = 218

Disaster Recovery Plans Are Widely Implemented

Which of the following items has your firm implemented to prepare for unforeseen outages (e.g. inclement weather, third-party issues, etc.)? (Select all that apply)



N = 218

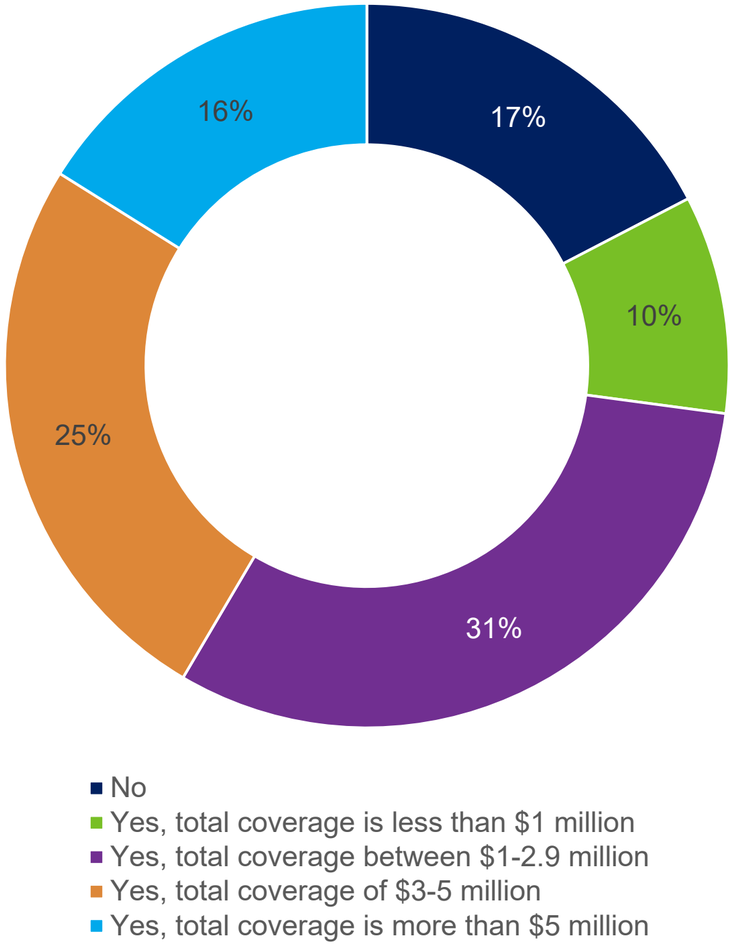
Cyber Insurance

Most Firms Have Some Cyber Insurance Coverage

Do you maintain cybersecurity insurance?

Analysis:

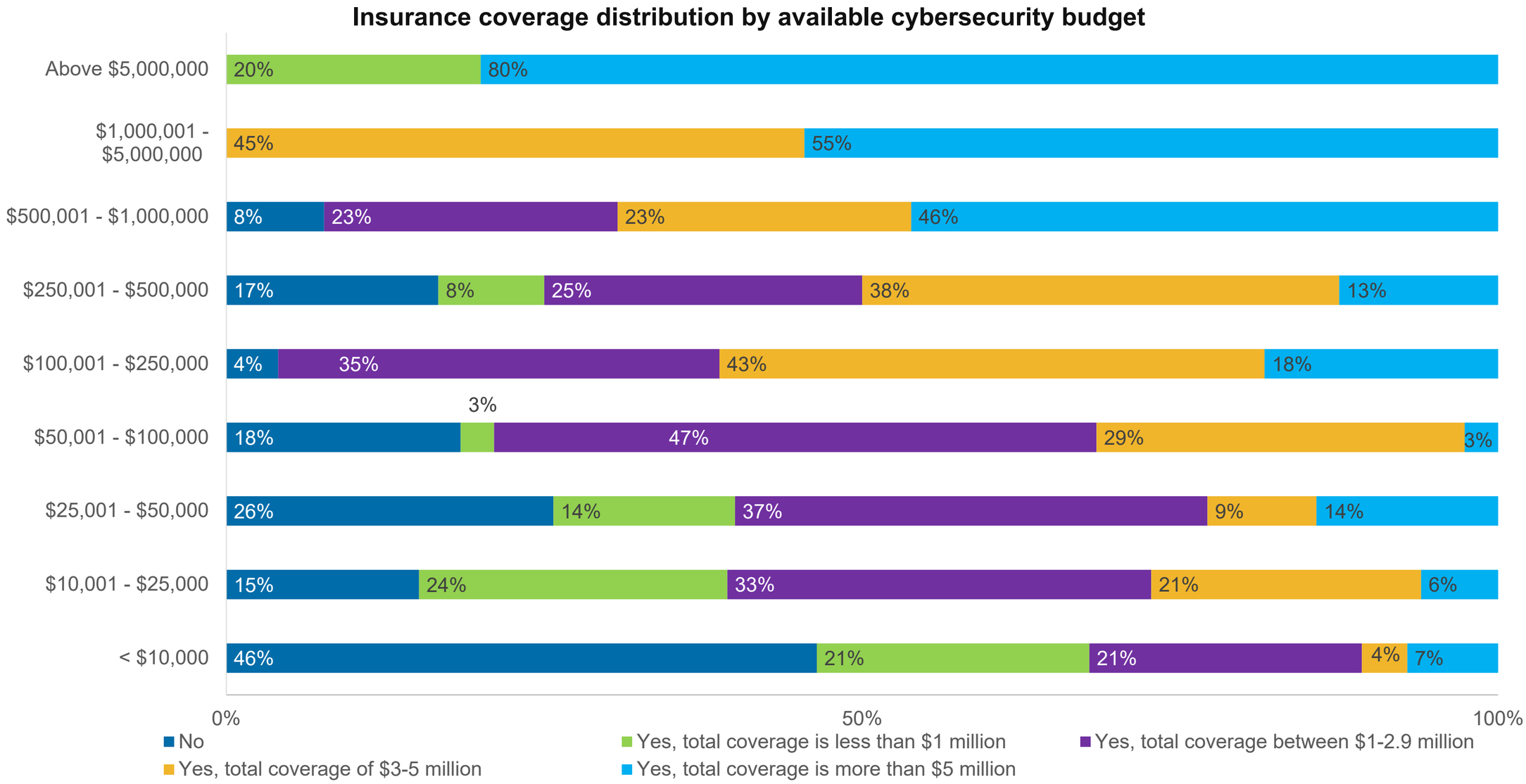
- Larger firms with greater cybersecurity budgets are most likely to maintain insurance coverage with higher limits.
- While **25%** of respondents overall indicated insurance coverage of $3-5 million, only **4%** of respondents with budgets of under $10,000 maintain that level of insurance coverage.
- **46%** of respondents with under $10,000 in cybersecurity budgets maintain no cybersecurity insurance.



N = 236

NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

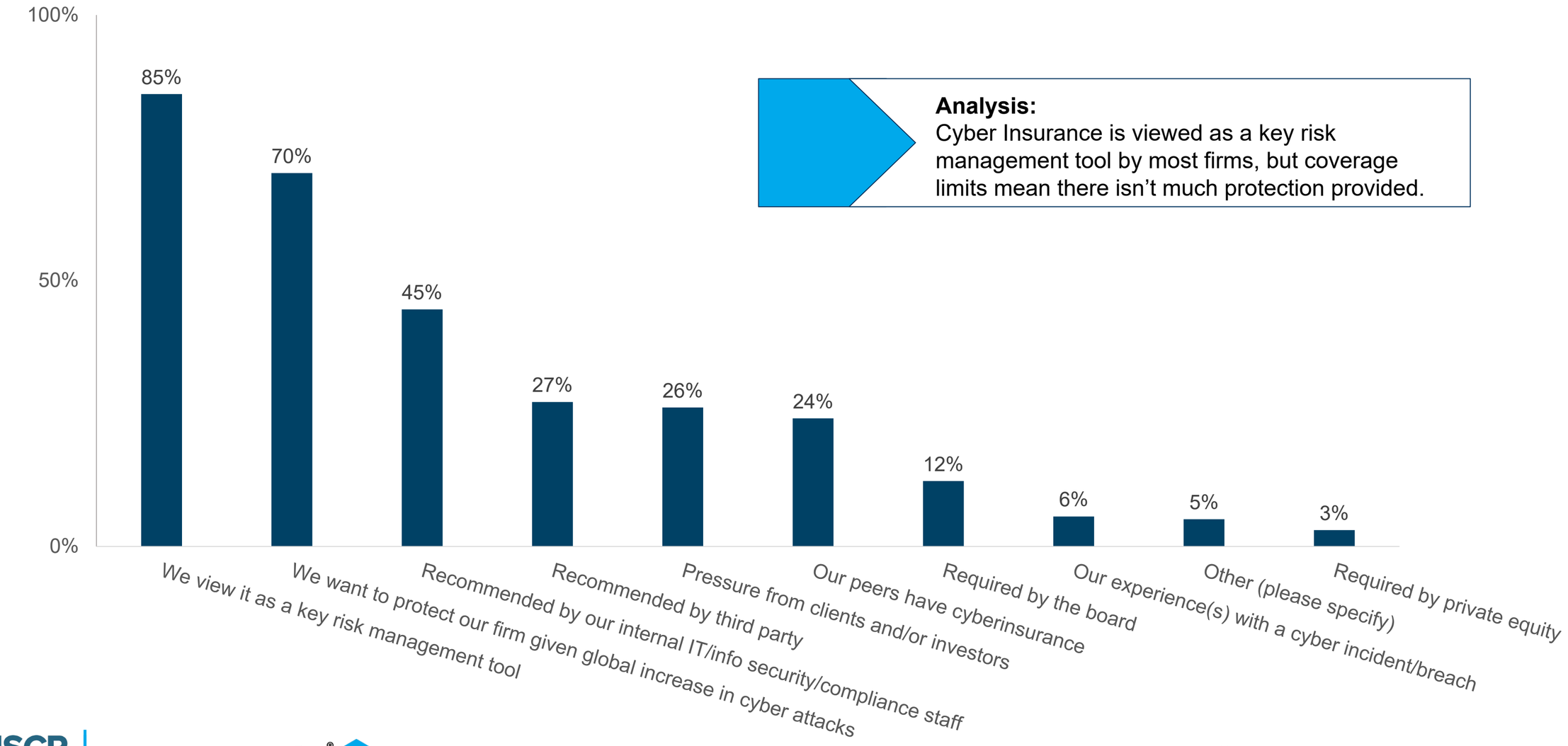
Cyber Insurance Can Be Limited by Budget



N = 236

Cyber Insurance Is Seen as Key Risk Management Tool

Which of the following factors influenced your decision to obtain cyber insurance coverage? (Select all that apply)



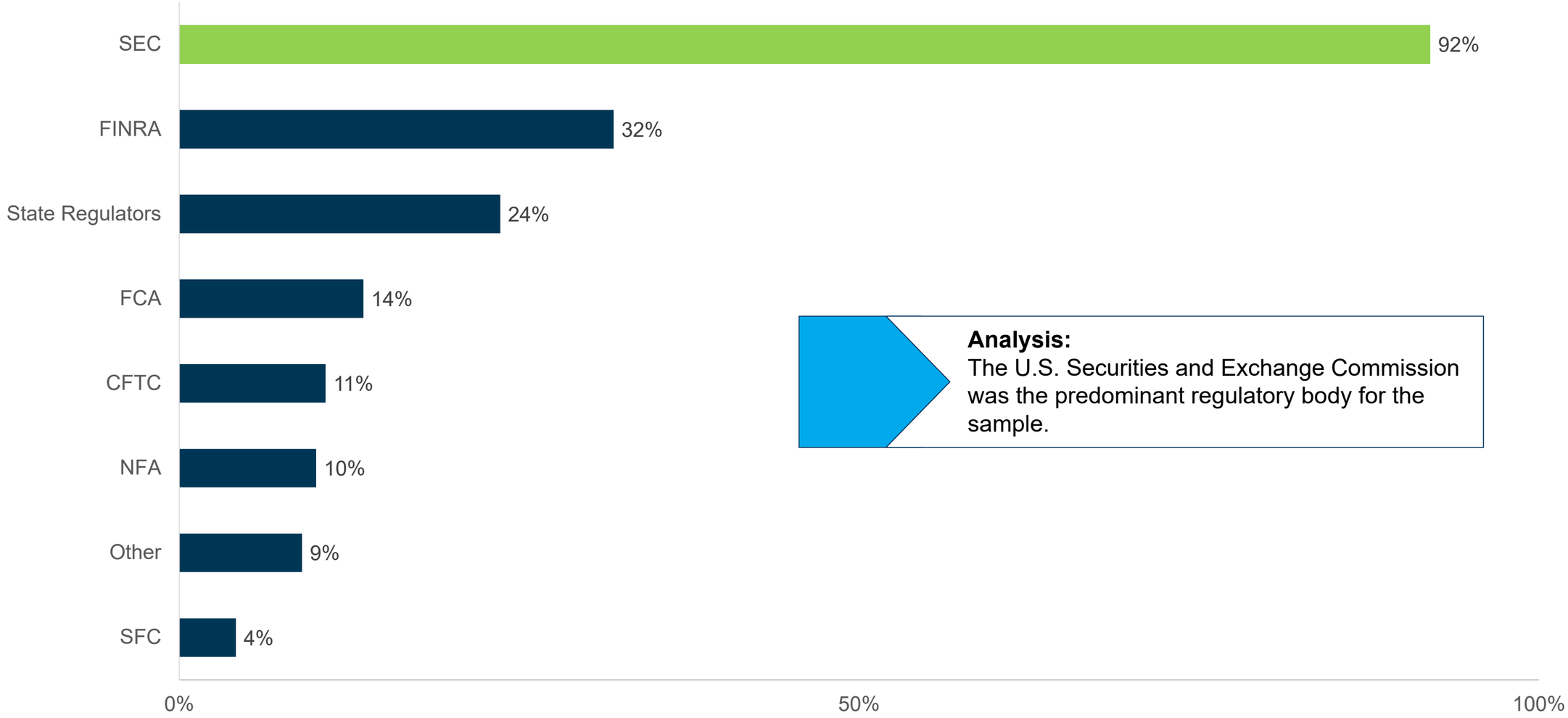
Analysis:
Cyber Insurance is viewed as a key risk management tool by most firms, but coverage limits mean there isn't much protection provided.

N = 195

Cybersecurity Regulations

Most Respondent Firms Are Regulated by the SEC

The regulatory bodies that oversee my firm include: (Select all that apply)

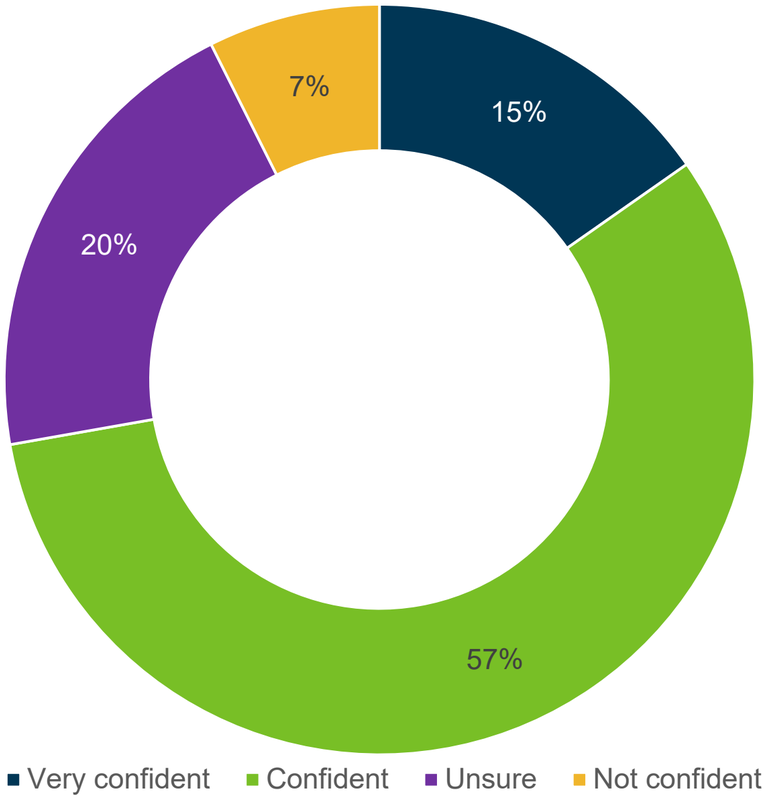


Analysis:
The U.S. Securities and Exchange Commission was the predominant regulatory body for the sample.

N = 288

Firms Express Confidence About Exams

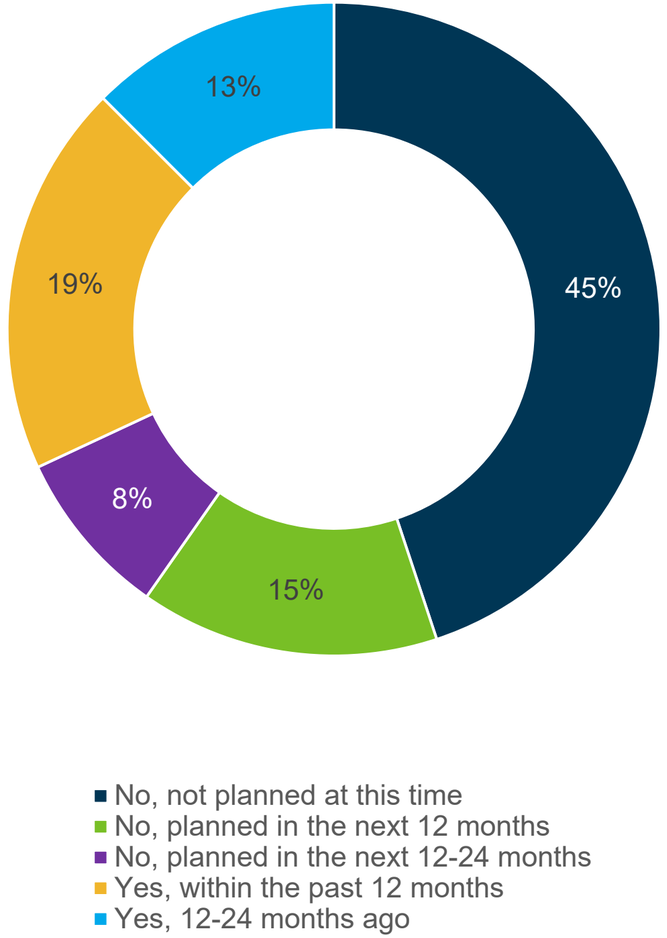
How confident are you in your organization's ability to undergo a cyber-focused exam by a regulator?



Analysis:
57% of firms are at least confident in their ability to get through a cyber-focused exam, but **45%** have not conducted mock examinations and have no plans of doing so within the next 24 months.

N = 216

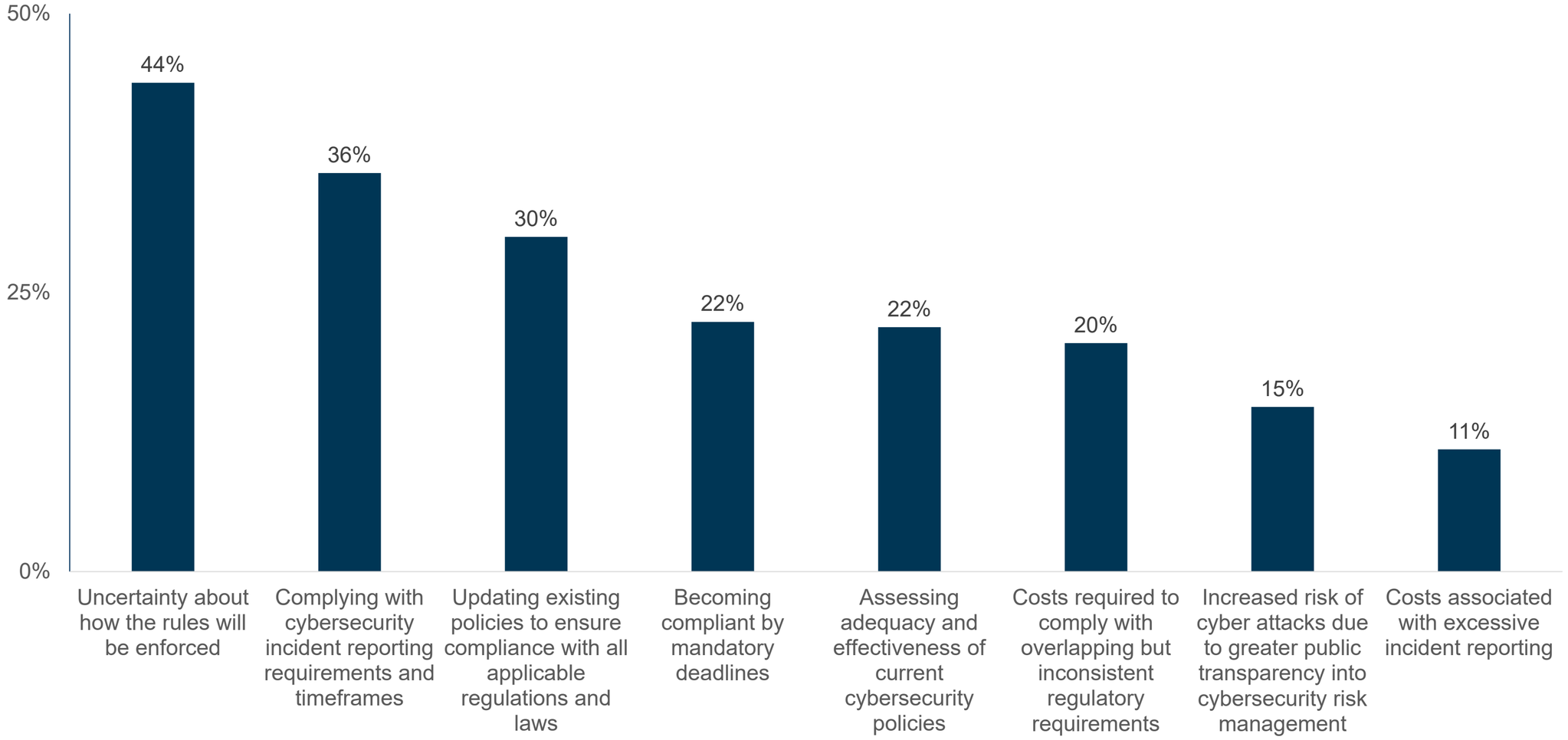
Have you conducted a mock regulatory cybersecurity examination?



NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

Firms Are Concerned About Rule Enforcement

What is most concerning to you about complying with the new SEC cybersecurity rules (e.g., public company incident disclosure rule, cybersecurity risk management for investment advisers, etc.) soon to take effect? (Select your two primary concerns)

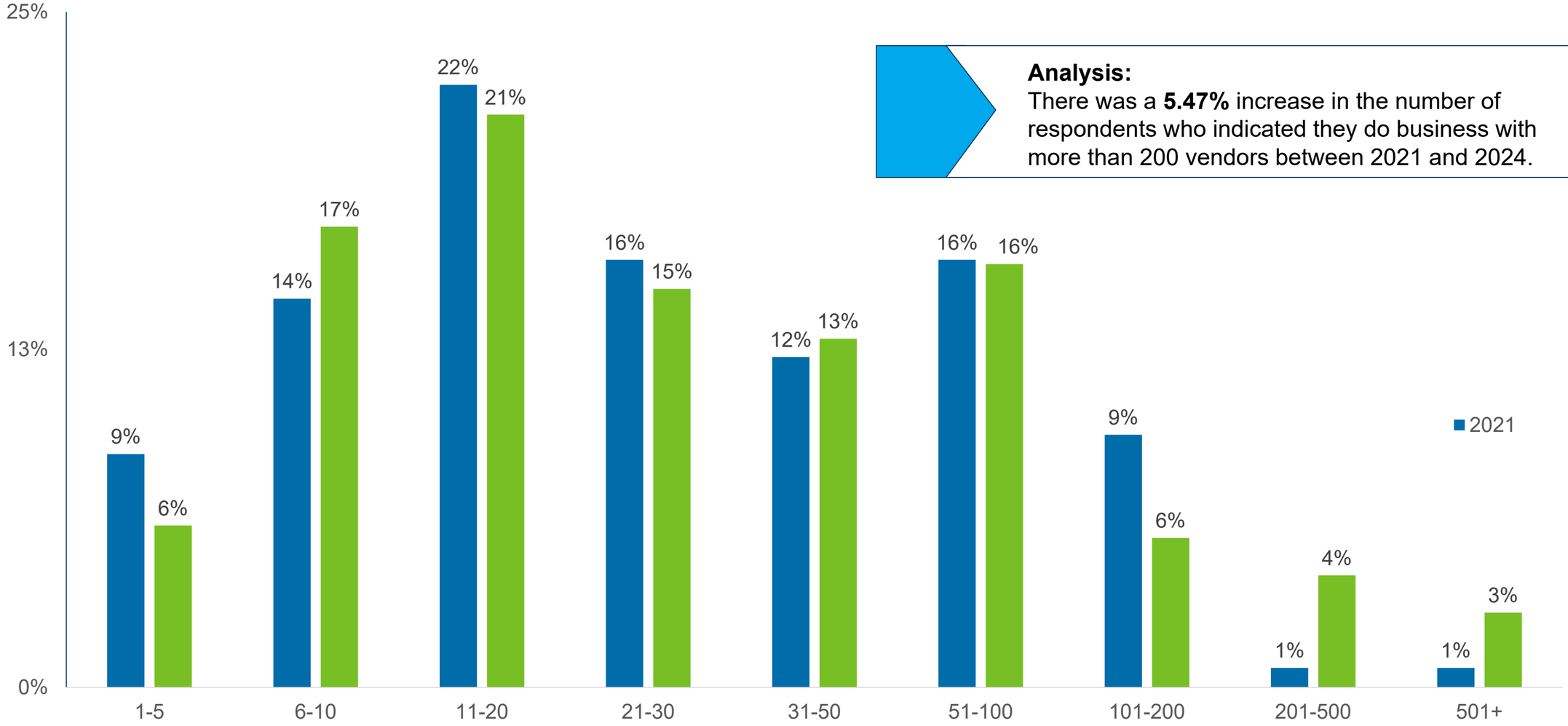


N = 210

Third-Party Risk Management

More Firms Rely on Large Number of Vendors

Approximately how many vendors do you do business with?



Analysis:
There was a **5.47%** increase in the number of respondents who indicated they do business with more than 200 vendors between 2021 and 2024.

2021 N = 139
2024 N = 217

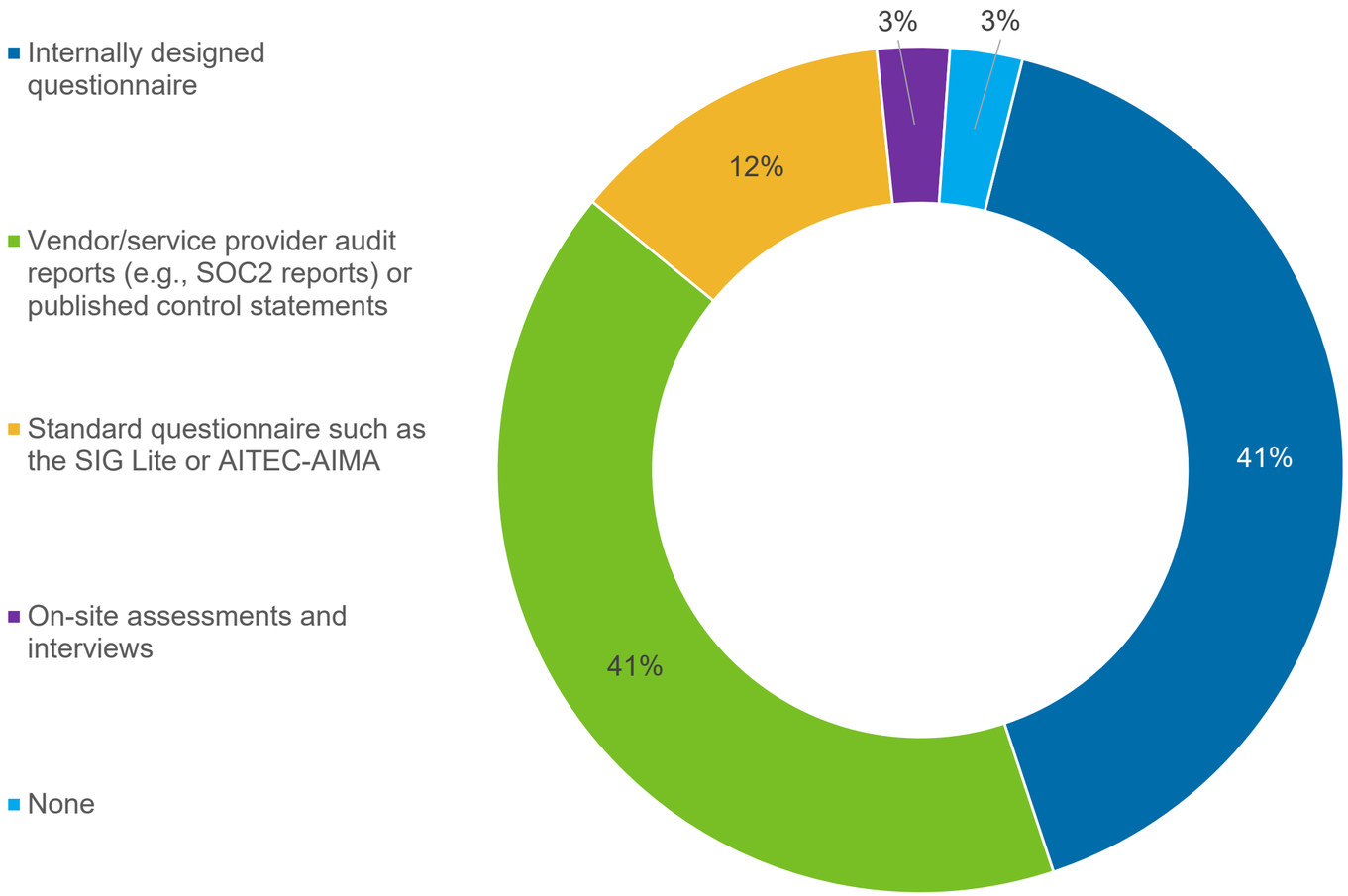
NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®

Questionnaires Are Key to Vendor Due Diligence

What is your primary approach to conducting vendor due diligence?

Analysis:

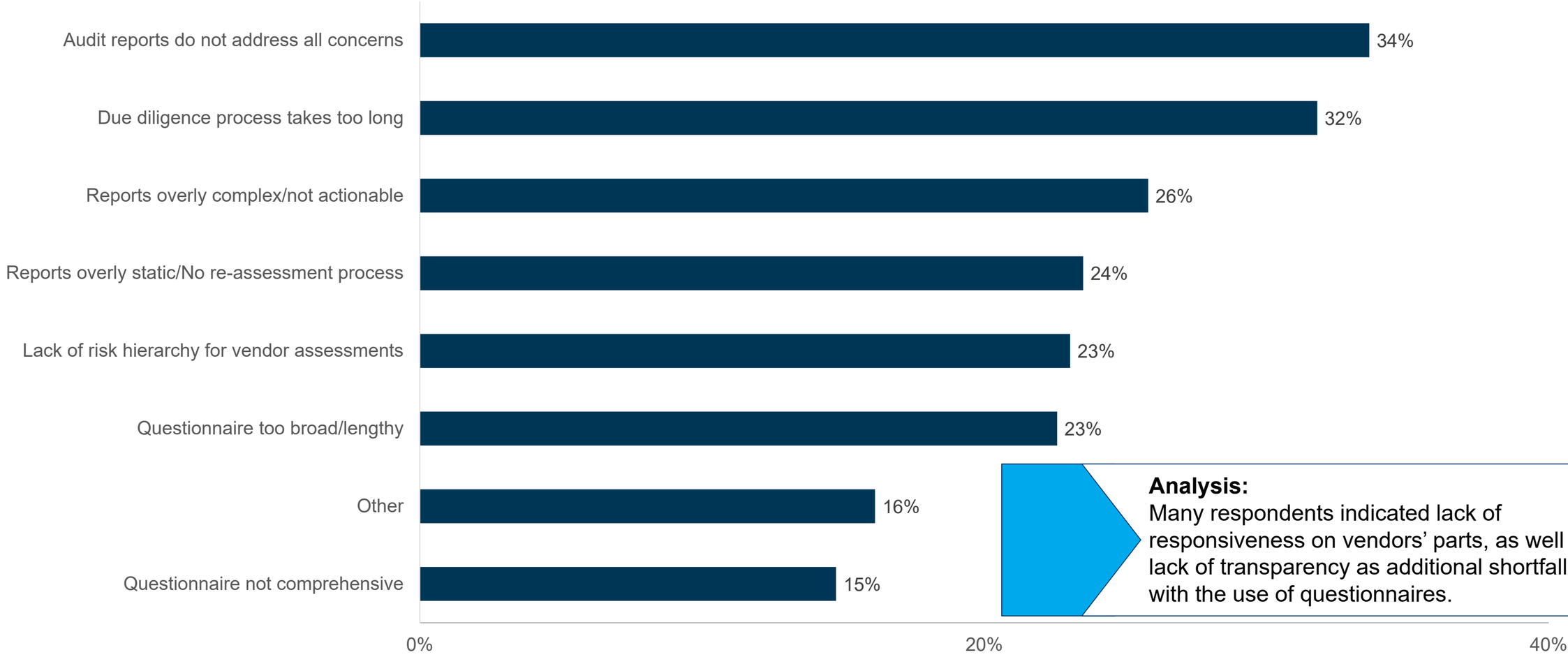
Over **80%** of firms indicated they rely on internally designed questionnaires or vendor audit reports and published control statements as their primary form of vendor due diligence.



N = 217

Vendor Due Diligence Proves Challenging to Firms

What are the shortfalls you associate with your primary approach to vendor due diligence? (Select all that apply)



Analysis:
Many respondents indicated lack of responsiveness on vendors' parts, as well as a lack of transparency as additional shortfalls with the use of questionnaires.

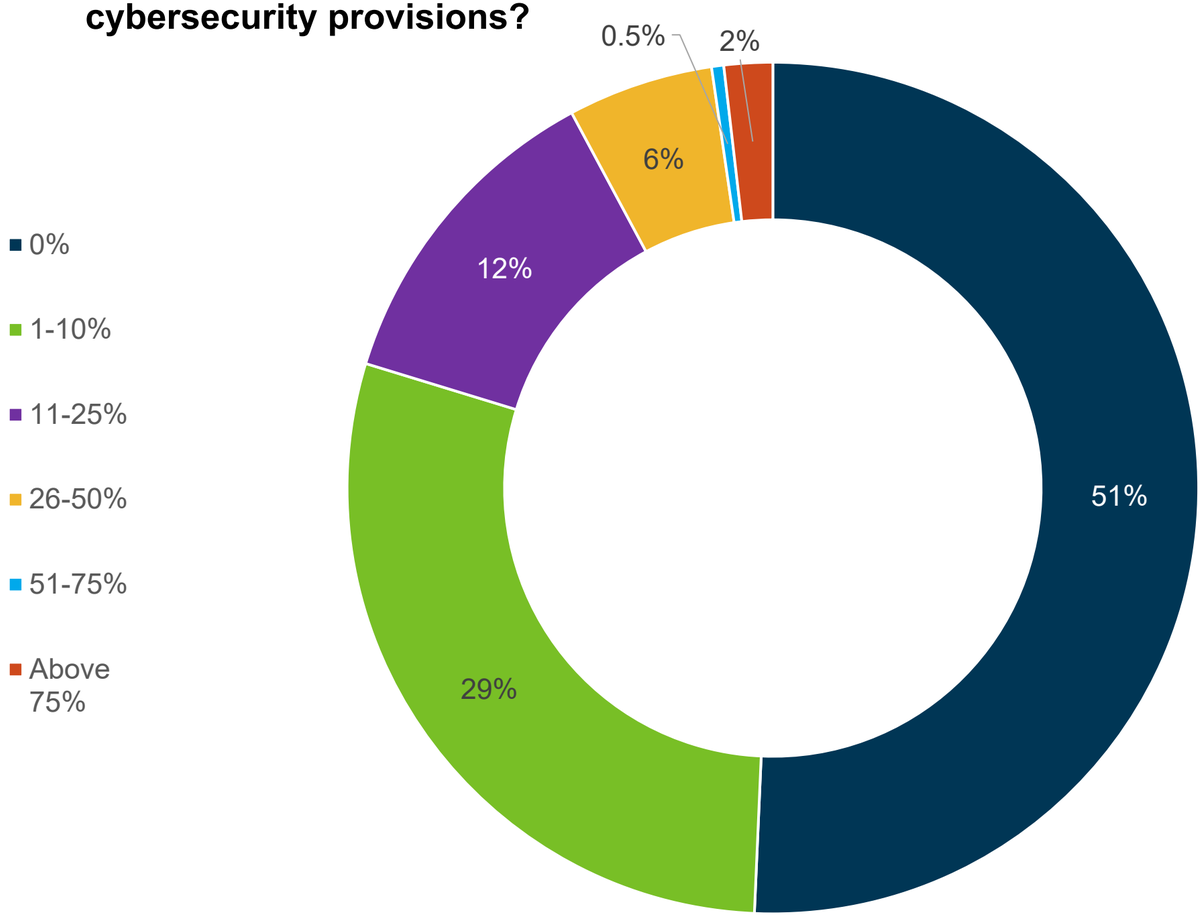
N = 217

Firms Don’t Usually Add Cybersecurity Provisions to Vendor Contracts

In the last 24 months, what percentage of your vendor contracts have you updated or renegotiated with additional cybersecurity provisions?

Analysis:

Despite clear concerns over how vendor due diligence is performed, over **50%** of firms have not renegotiated any vendor contracts with additional cybersecurity provisions.



N = 217

AI Risk Management

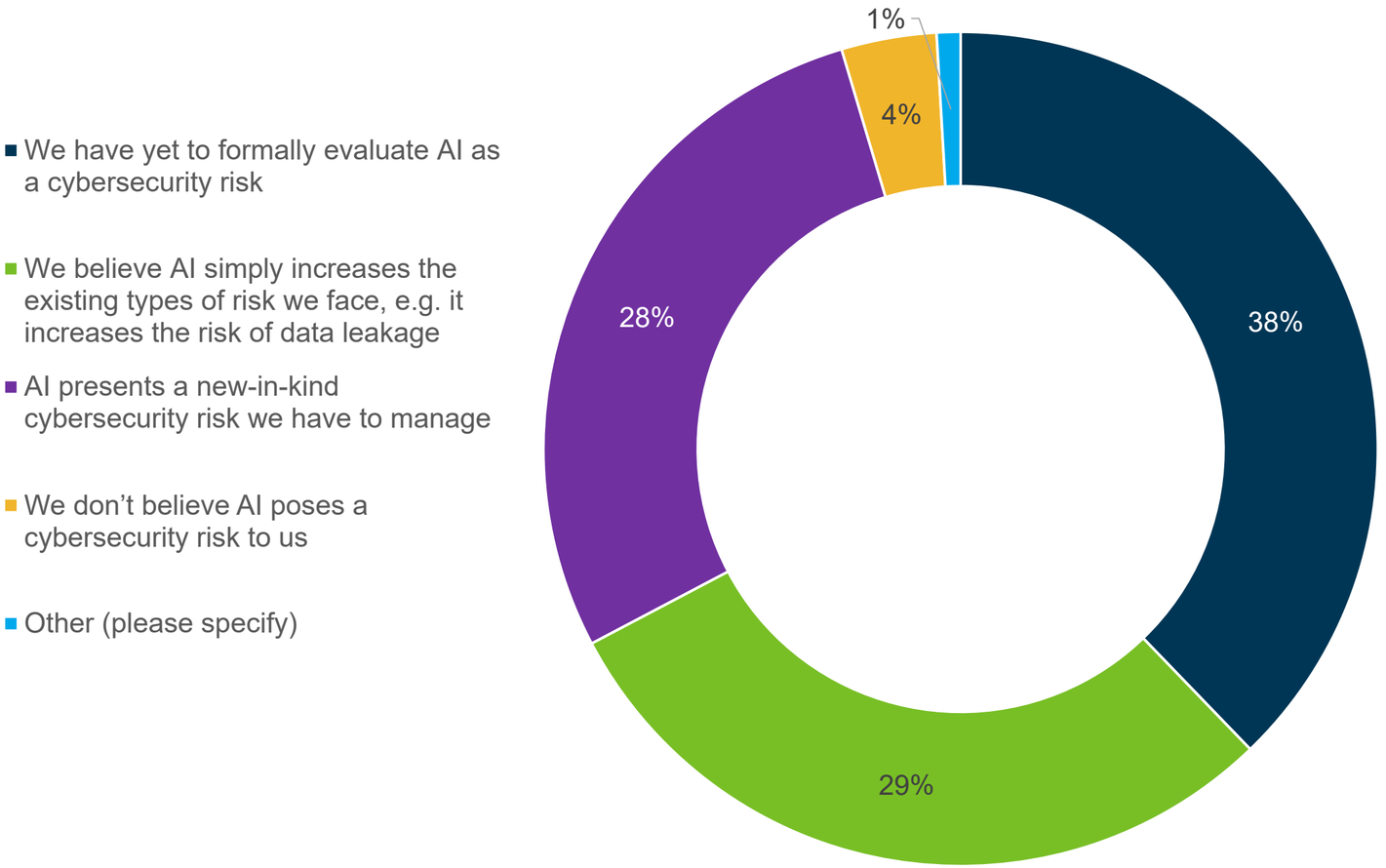
AI Is Slow to be Understood as a Cybersecurity Risk

How is your firm considering AI as a cybersecurity risk? Please choose the option that most closely describes your thinking.

Analysis:

Nearly **40%** of respondents have yet to evaluate AI as a cybersecurity risk.

58% of respondents indicated they see AI either as a new cybersecurity risk or a factor increasing existing risks.



N = 217

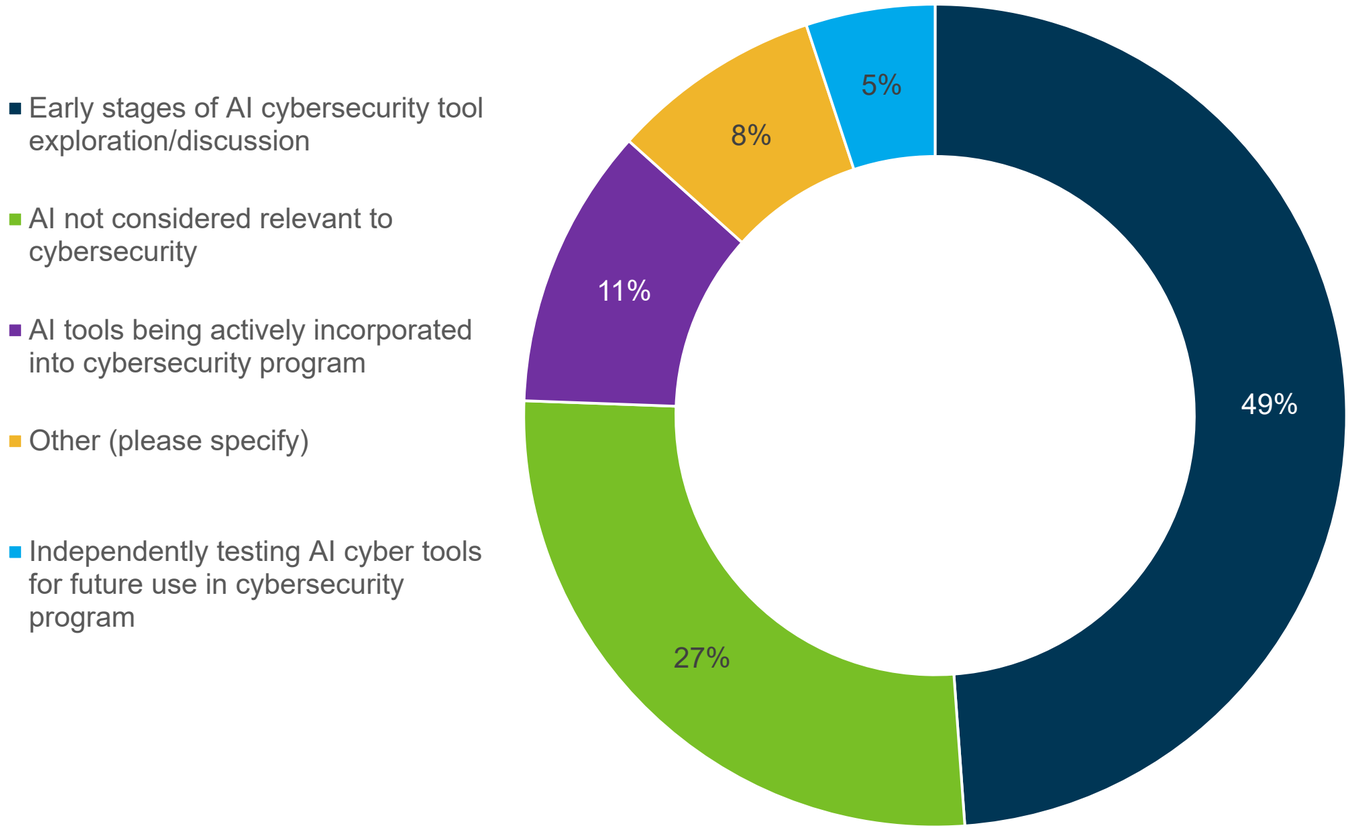
AI Is Not Yet Broadly Pursued as a Cybersecurity Tool

How is your firm incorporating AI as a tool into cybersecurity risk management practices?

Analysis:

Incorporating AI into cybersecurity can be influenced by a firm's budget.

Less than **10%** of firms with budgets under $10,000 indicated AI tools were being actively incorporated into their cybersecurity programs, as opposed to **30%** of firms with budgets between $1 million and $5 million

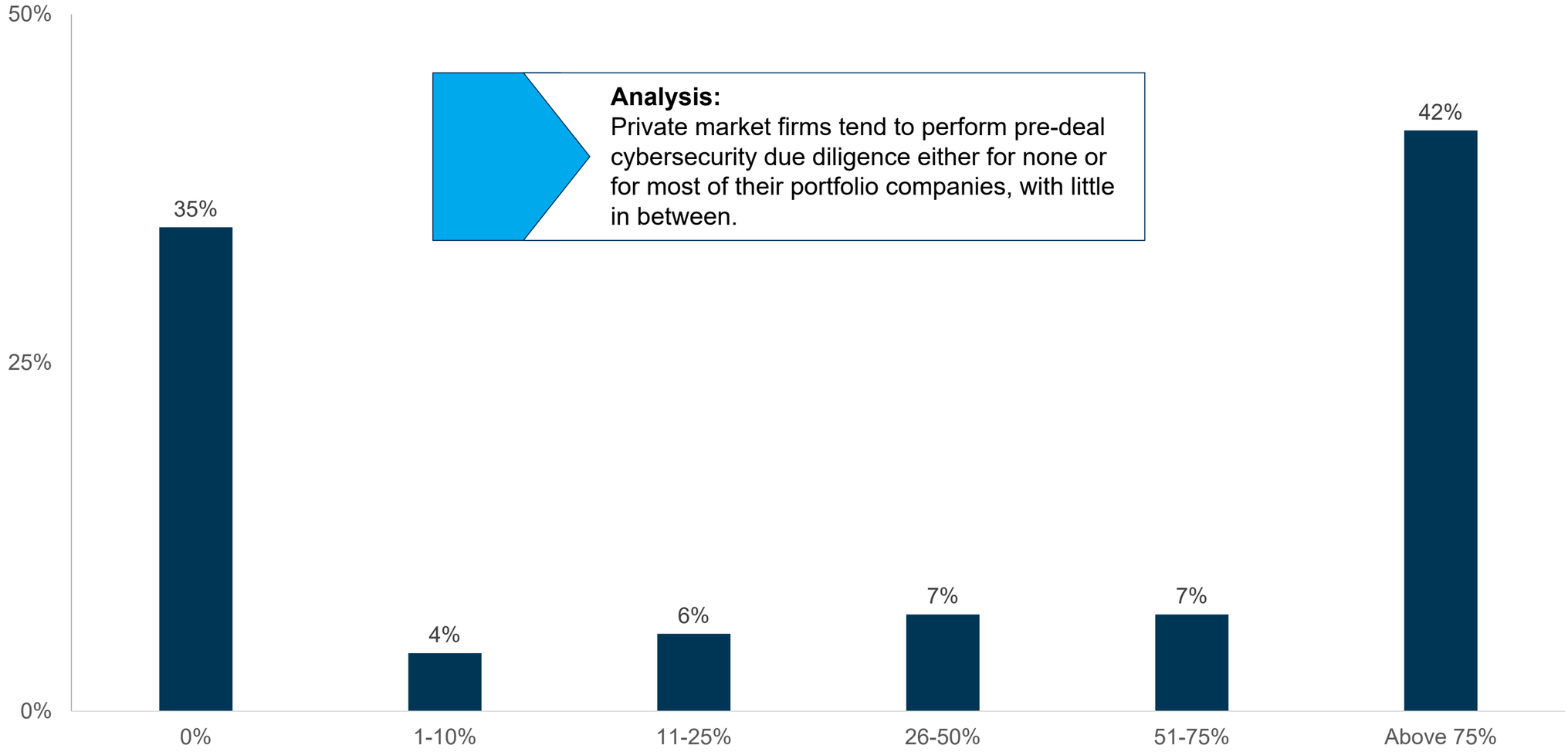


N = 217

Portfolio Company Risk Management

Pre-Deal Due Diligence Is Not a Balanced Practice

What percentage of your portfolio companies have you conducted cybersecurity diligence on before investment?

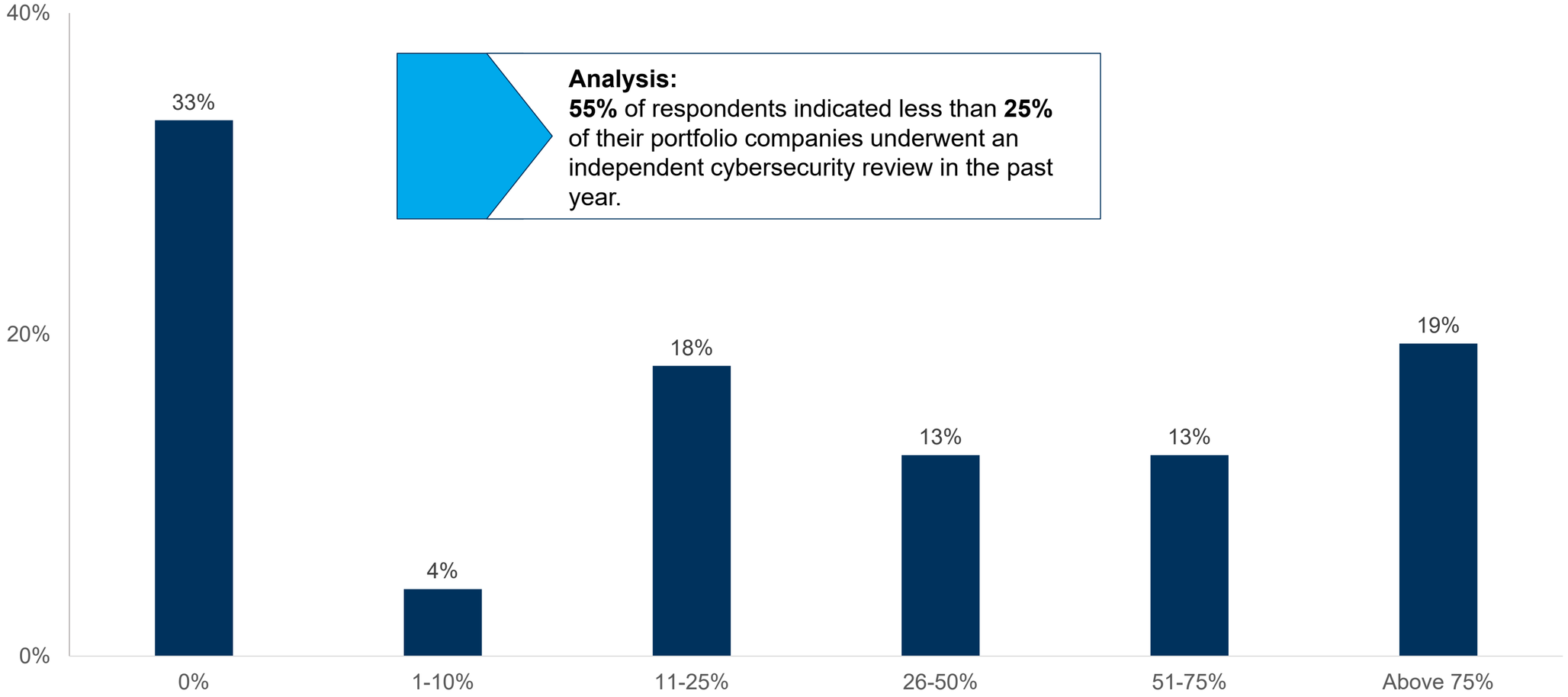


Analysis:
Private market firms tend to perform pre-deal cybersecurity due diligence either for none or for most of their portfolio companies, with little in between.

N = 72

Independent Cybersecurity Reviews Are Not Extensively Performed

What percentage of your portfolio companies have undergone independent cybersecurity reviews in the previous 12 months?

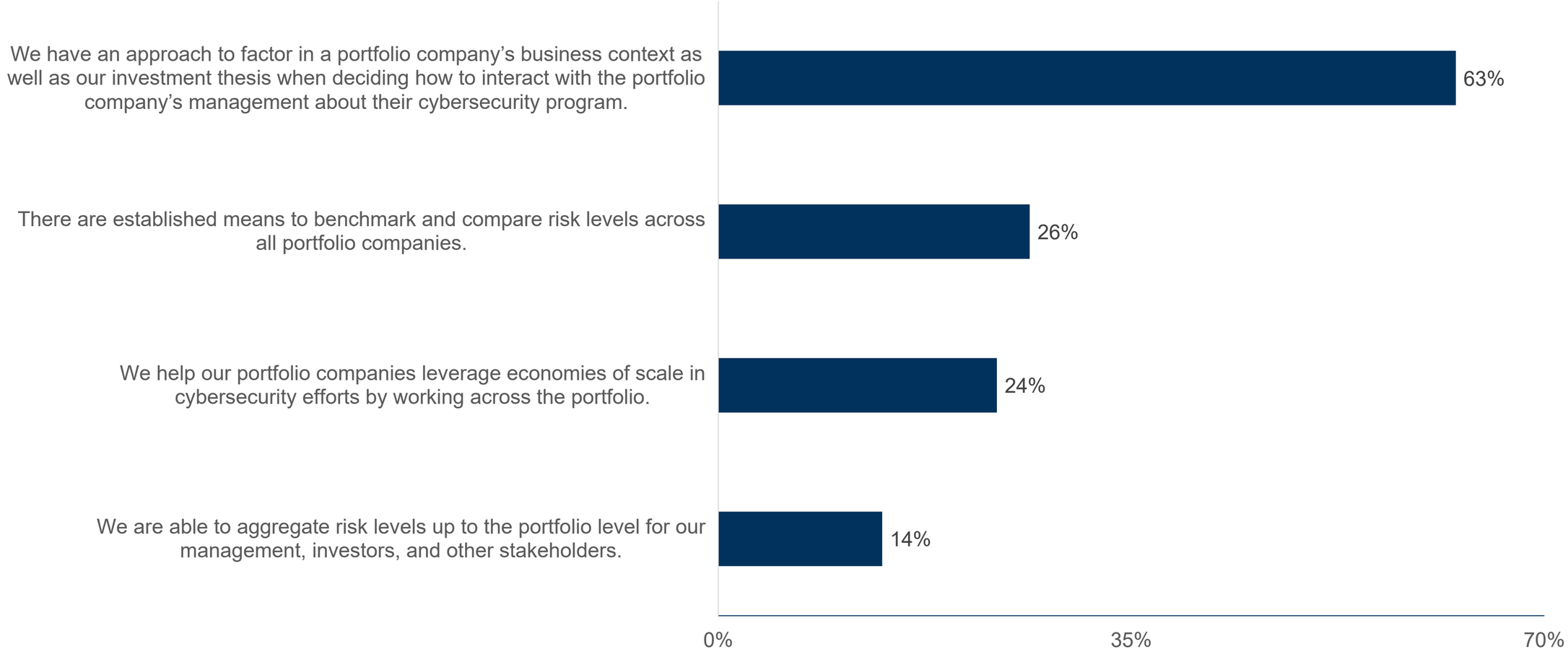


Analysis:
55% of respondents indicated less than **25%** of their portfolio companies underwent an independent cybersecurity review in the past year.

N = 72

Cybersecurity Oversight Is Limited In Capability

Which of the following capabilities does your cybersecurity oversight program have across your portfolio of companies? (Select all that apply)



N = 72

About ACA Aponix

ACA Aponix, a division of ACA Group, provides cybersecurity risk assessments, data privacy compliance services, vendor and M&A diligence services, portfolio company oversight, network testing, and advisory services for companies of all sizes. Our award-winning solutions are designed to help firms uncover risks and identify deficiencies in their cybersecurity policies, procedures, and controls.

Visit us at www.acaglobal.com to learn more or contact our team below.

Contact us

About NSCP

Since 1986, the National Society of Compliance Professionals has been the leading non-profit, membership organization dedicated to supporting compliance professionals in the financial services industry, focusing primarily on investment advisers, broker-dealers, and private funds. NSCP membership offers a wide range of compliance resources, educational opportunities, and regulatory advocacy and engagement.

Visit us at nscp.org to learn more or contact our team below.

Contact us

NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS | ACA Aponix®