FPA FINANCIAL PLANNING ASSOCIATION

RESEARCH & PRACTICE INSTITUTE™

Sponsored by TD Ameritrade Institutional

Is Your Data Safe?

The 2016 Financial Adviser Cybersecurity Assessment

Table of Contents

Welcome 3

Executive Summary 4

Introduction and Methodology 6

Preparation and Readiness 8

- Client Awareness and Concern 11
- Investing in Cybersecurity 12

Execution: Policies and Procedures 14

- Governance and Risk Assessment 15
- Access Rights and Controls 19
- Data Loss Prevention 23
- Vendor Management 26
- Incident Response 29
- Training 33

Appendix 1 – Participant Profile 36

Appendix 2 – Detailed Results by Segment 40

In today's fast-paced digital world, data security is paramount—especially in the financial services arena where there are many questions to consider. Have financial advisers taken the necessary steps to safeguard their business and client data? What have they done to prepare for the risks associated with cyberattacks and what are the key gaps in practices today relating to cybersecurity?

These and other issues are the focus of *Is Your Data Safe? The 2016 Financial Adviser Cybersecurity Assessment*, the latest research from the FPA Research and Practice Institute™, sponsored by TD Ameritrade Institutional.

This report aims to help you understand what precautions your peers are taking against cyberattacks and where they are falling short. The report is purely quantitative, to give you the metrics you need to see how you and your business stack up compared to your peers. Additionally, this fall, we will introduce a series of whitepapers that will further dig into the data and offer actionable next steps that you can apply to your business. The whitepapers will answer the following questions:

- How are advisers communicating with clients regarding cybersecurity?
- How are advisers training their teams on issues related to cybersecurity?
- What tools and technology are advisers using to protect their businesses—and what does it cost?

Enjoy the *Is Your Data Safe? The 2016 Financial Adviser Cybersecurity Assessment* and stay tuned for more practice management content coming soon.

LAUREN M. SCHADLE, CAE
CEO/Executive Director
Financial Planning Association

TOM NALLY
President
TD Ameritrade Institutional

Executive Summary

The issue of cybersecurity is as complex as it is important. While a majority of advisers agree that protecting their firms and their clients is a key priority, many don't feel completely prepared.

This new research from the FPA Research and Practice Institute™, sponsored by TD Ameritrade Institutional, gets below the surface of this critical issue to examine both perception and action. Advisers shared in-depth information on exactly how they are preparing their firms, where there are gaps, how they are training their teams, how they are communicating with clients and the tools they are using to take action.

This initial quantitative report provides an in-depth examination of where advisers are today and will be followed by a series of whitepapers that provide actionable takeaways.

Among the key findings of this initial analysis is the following:

Perception and Readiness

- Cybersecurity continues to be an important priority
  - 81 percent of respondents indicate this is a high or very high priority
- While overall respondents believe they understand the issues associated with cybersecurity, many see room for improvement
  - 44 percent of respondents 'completely agree' that they fully understand the issues and risks associated by cybersecurity. That drops to 36 percent when they reflect on their team's understanding.
- The understanding of the specific requirements as set forth by OCIE (Securities and Exchange Commission's Office of Compliance Inspections and Examinations) is relatively low.
  - 26 percent of respondents say they 'completely agree' that they are aware of all of the requirements.
  - Respondents acknowledge that there is still work to be done
- Lower awareness is impacting confidence
  - 29 percent of respondents say they 'completely agree' that they are fully prepared to manage and mitigate the risks associated with cybersecurity.
- Only 18 percent of respondents are 'very confident' they would pass an OCIE examination today.

Execution

The study asked respondents about the extent to which they had formally documented policies and procedures related to the six key cybersecurity areas.

- Respondents consider governance/risk assessment, vendor management and data loss prevention the most challenging elements of creating an overall cybersecurity plan.
- The proportion of firms with documented plans and procedures in place ranged depending on the specific element of cybersecurity. Below are the percentages of respondents who indicated the firm had documented policies and procedures in place for each of the following:
  - Governance and Risk Assessment **57%**
  - Access Rights and Controls **59%**
  - Data Loss Prevention **58%**
  - Vendor Management **43%**
  - Incident Response **43%**
  - Training **51%**

The report goes deeper into each element to highlight gaps within each area and plans to close those gaps.

Introduction and Methodology

Tackling a subject as broad as 'trends in practice management' is no small challenge. According to the 2016 TD Ameritrade Institutional RIA Sentiment Survey, cybersecurity is the number one priority for RIAs. The issue is front and center in the media, at conferences and in hallway discussions among advisers.

Like you, other advisers recognize the critical importance of ensuring that company and client data is secure, but it's a complex issue that will only continue to grow in complexity. There are many factors that must be considered when protecting your firm and clients from cyberattacks; having the right policies and procedures in place is just the beginning.

This new research from the FPA Research and Practice Institute™, sponsored by TD Ameritrade Institutional, gets below the surface of this critical issue to examine both perception and action. Advisers shared in-depth information on exactly how they are preparing their firms, where there are gaps, how they are training their teams, how they are communicating with clients and the tools they are using to take action.

This Report:

This initial report focuses on the data. On the following pages, you will find both high-level perceptions and an in-depth assessment of where the industry sits across key components of cybersecurity, including:

- Governance and Risk Assessment
- Access Rights and Controls
- Data Loss Prevention
- Vendor Management
- Incident Response
- Training

In the first section, you'll find a summary of all responses. More importantly, Appendix 2 includes a detailed presentation of the same questions, providing the full breakdown of responses and across key respondent segments including: role, assets under management, gross revenue and team size. This report is designed to provide the facts, but without interpretation. An upcoming series of whitepapers will offer insights, interpretation and actionable takeaways.

The Whitepapers:

FPA, with TD Ameritrade Institutional, will release a series of whitepapers in the fall of 2016 that will focus on specific issues relating to cybersecurity and will include actionable takeaways. They will answer three key questions:

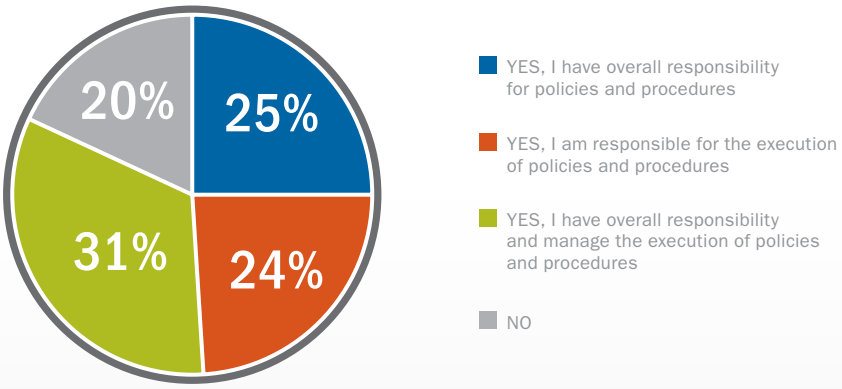
1. **Whitepaper #1: How are advisers communicating with clients regarding cybersecurity?**
2. **Whitepaper #2: How are advisers training their teams on issues related to cybersecurity?**
3. **Whitepaper #3: What tools and technology are advisers using to protect their businesses—and what does it cost?**

Methodology

This report incorporates feedback from 1,015 respondents from across the country, including FPA members and non-members as well as advisers who custody with TD Ameritrade Institutional. The majority of respondents are RIAs. For a full participant profile, please see Appendix 1.

Participants responded to an online survey conducted in June–July 2016, taking approximately 15 minutes to complete. The study's overall margin of error is +/- 3.07percent.

Respondents included those who had overall responsibility for policies and procedures, those who had executional responsibility and those who had both. The breakdown is below and the in-depth questions relating to the specifics of what is being done was asked of the 55 percent of advisers who had a role in execution.

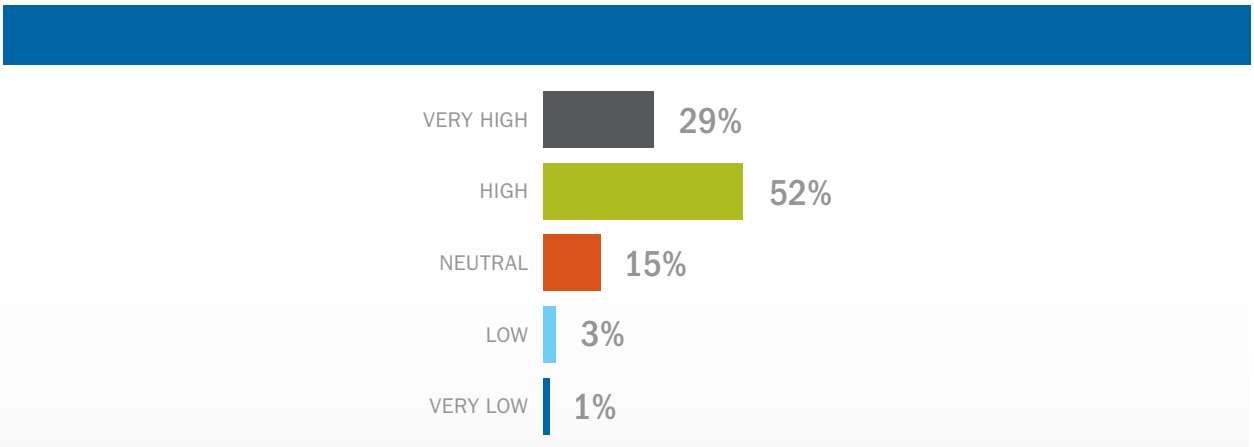


Q: *Are you responsible for risk management and procedures at your firm?*

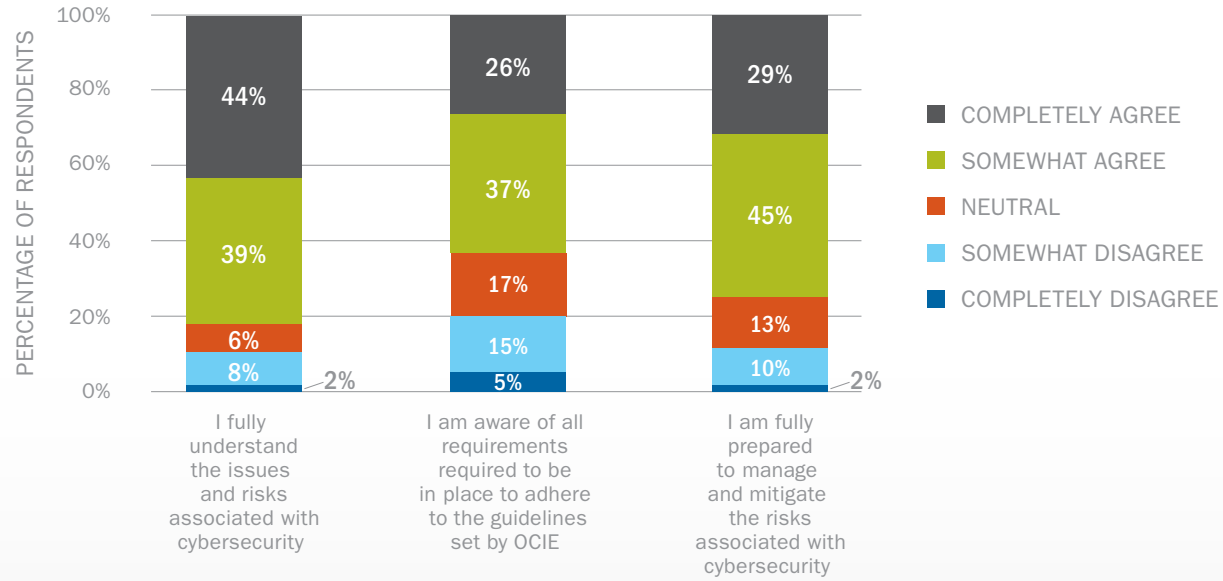
Perception and Readiness

We know that advisers consider cybersecurity a critical issue for their firms with 81 percent rating this issue as high or very high among their priorities.

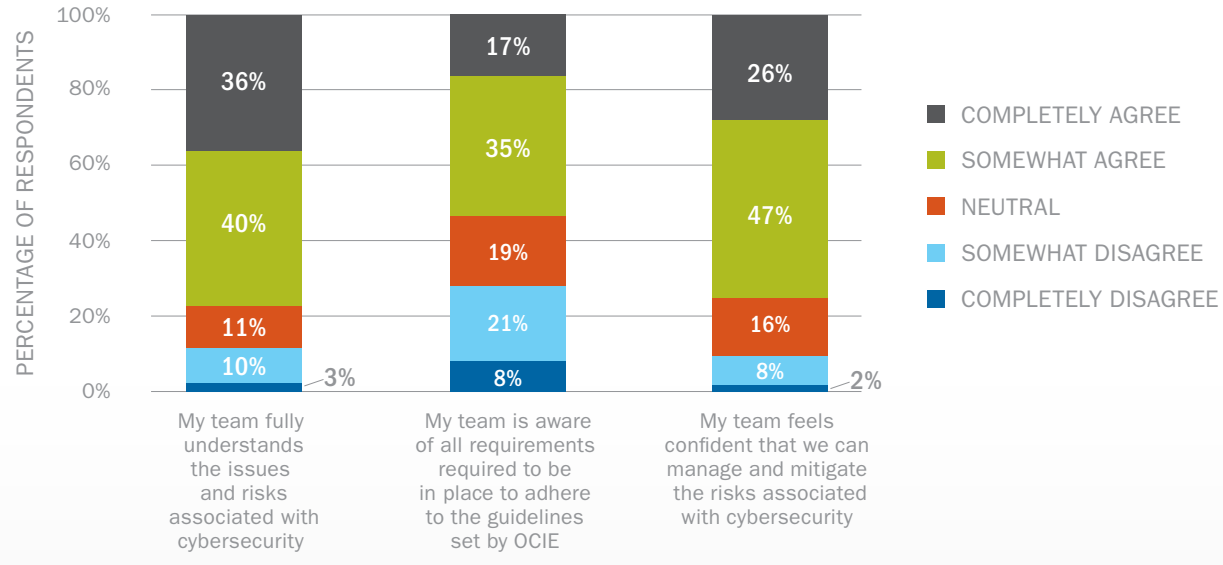
Despite being a high priority, not all advisers believe they are yet fully prepared to mitigate the risks as outlined by the Office of Compliance Inspections and Examinations (OCIE). This is a considerably bigger issue among team members who are not directly responsible for execution and, as a result, overall confidence in passing an OCIE exam is relatively low.



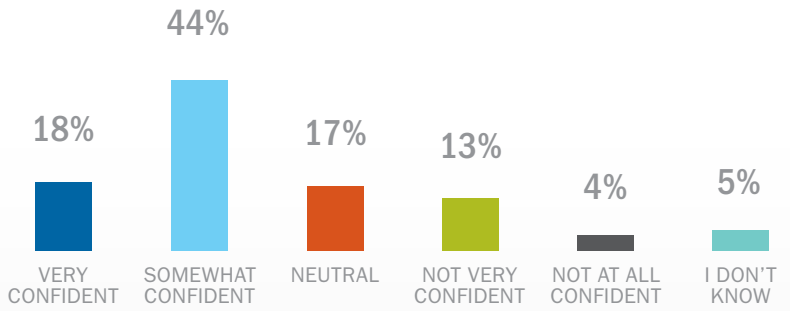
Q: *How would you describe where cybersecurity ranks amongst your firm's priorities?*



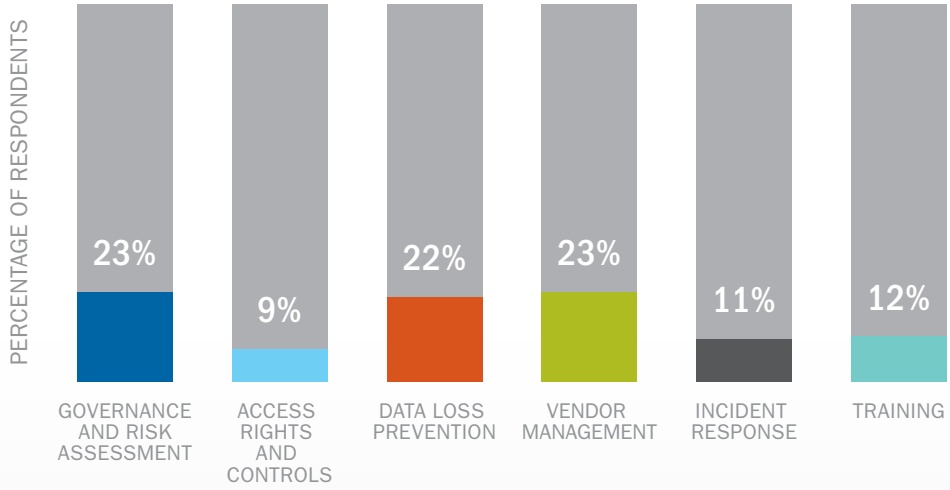
Q: *To what extent do you agree or disagree with the following statements:*



Q: *To what extent do you agree or disagree with the following statements as they relate only to the other members of your team and not yourself?*



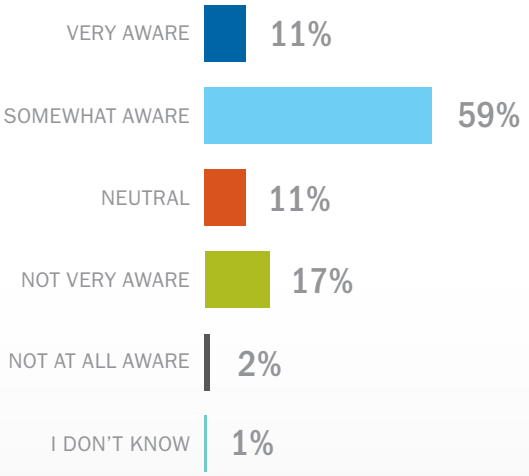
Q: *If you were to undergo an OCIE cybersecurity examination today, how confident are you that you would pass?*



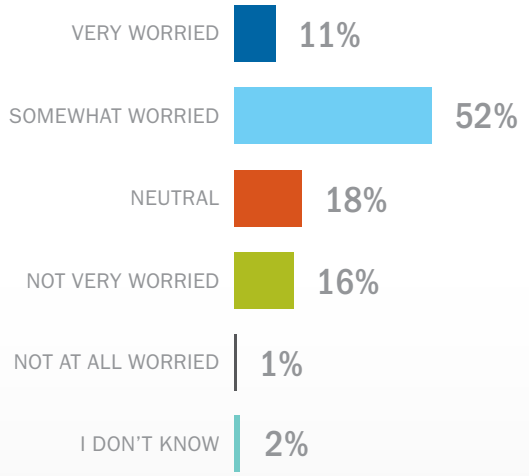
Q: *Which elements of creating an overall cybersecurity plan do you consider the most challenging to implement? (n=those who had completed work in all relevant areas)*

Client Awareness and Concern

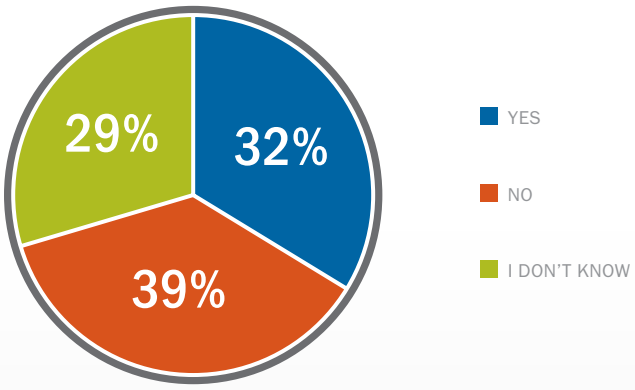
According to advisers, they believe their clients are only somewhat aware of the risks associated with data security. This perceived lack of awareness likely contributes to the perception that clients are not particularly worried about the issue.



Q: *To what extent do you think your clients are aware of the risks associated with data security?*



Q: *To what extent do you think your clients are worried about security breaches with respect to their data?*



Q: *Do you feel your approach to dealing with cybersecurity risks is a competitive advantage relative to other advisers?*

Investing in Cybersecurity

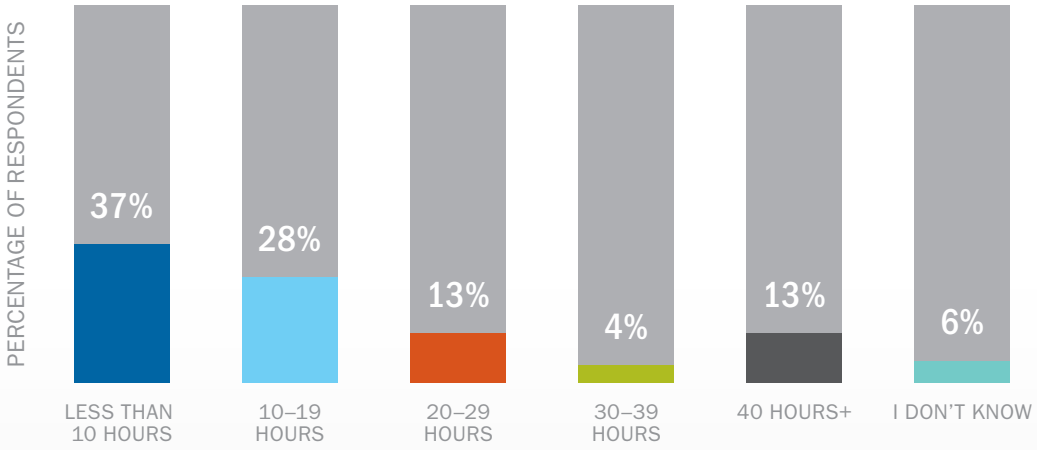
There is a significant range in the dollars and time invested in cybersecurity, which relates both to firm size and the extent to which the issue is a priority.

We have not invested externally	23%
Less than $5,000	37%
$5,000 – $9,999	12%
$10,000 – $14,999	4%
$15,000+	6%
I don't know	19%

Q: *How much have you spent externally in the last 12 months, in total, in order to define or implement policies and procedures related to cybersecurity (i.e. consultants, third party vendors, etc.)?*

We have not invested internally	21%
Less than $5,000	44%
$5,000 – $9,999	8%
$10,000 – $14,999	3%
$15,000+	5%
I don't know	19%

Q: *How much have you invested in internal resources in the last 12 months, in total, in order to define or implement policies and procedures related to cybersecurity (i.e. new hires, education, etc.)?*



Q: *In the last year, how much time have you personally invested in understanding or managing the implementation of policies and procedures related to cybersecurity?*

Execution: Policies and Procedures

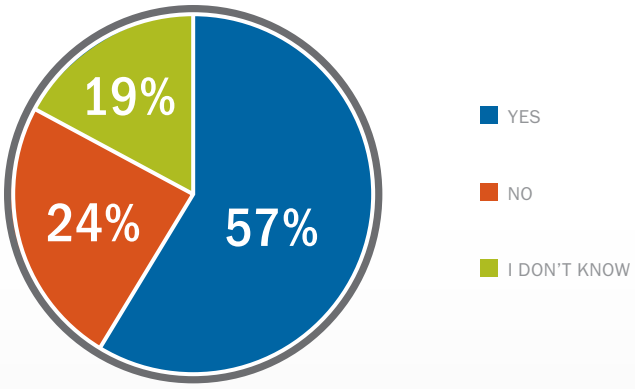
On the following pages, we go deeper on each of the six key areas associated with cybersecurity.

- Governance and Risk Assessment
- Access Rights and Controls
- Data Loss Prevention
- Vendor Management
- Incident Response
- Training

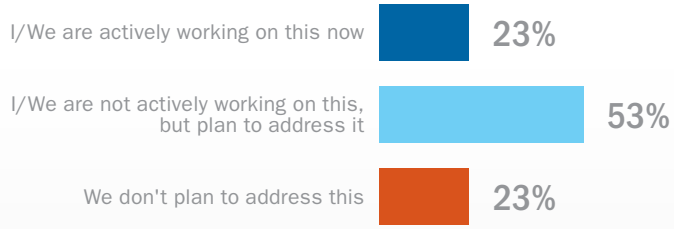
These questions were only asked of the 55 percent of respondents who had **executional responsibility** for the development or implementation of policies and procedures.

Governance and Risk Assessment

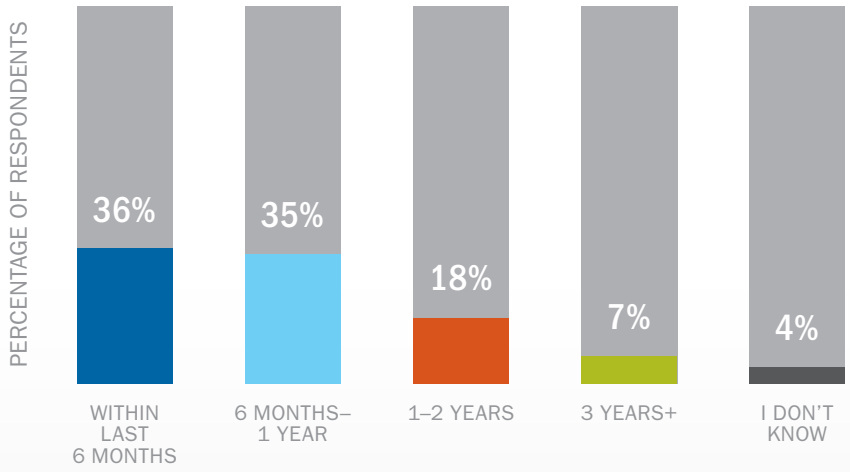
Nearly 60 percent of respondents indicated they had formally documented policies and procedures related to governance and risk assessment. Respondents were asked detailed questions on exactly how they are preparing across a range of issues associated with this overall category.



Q: *Do you have policies and procedures formally documented today as it relates to governance and risk assessment?*



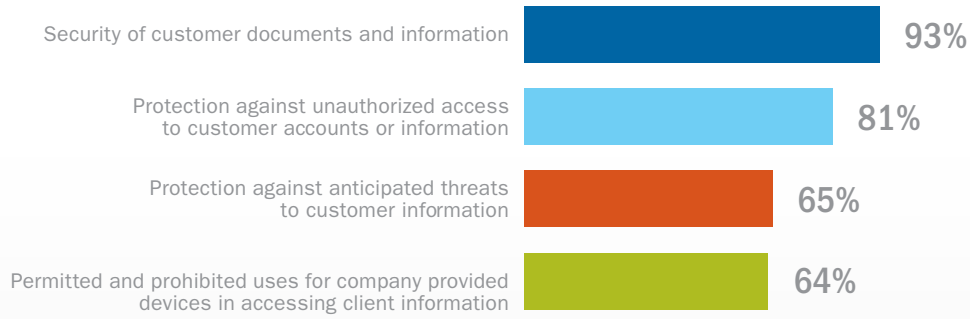
Q: *What are your plans related to documenting policies and procedures for governance and risk assessment? (n=those who do not have policies and procedures in place related to governance and risk assessment)*



Q: *When was the bulk of that work completed?*
(n=those who have policies and procedures in place related to governance and risk assessment)

Protection of client records and information	85%
Periodic risk assessments	64%
Firm's organizational structure (specifically positions responsible for cybersecurity-related matters)	59%
Chief Information Security Officer (or equivalent) or other employees responsible for cybersecurity matters	48%
Vulnerability scans and any remediation efforts	37%
Patch management practices (e.g., prompt installation and documentation of critical patches)	34%
Penetration testing (conducted by or on behalf of the firm) including remediation efforts	21%
I don't know	8%
None of the above	1%

Q: *For which of the following do you have formally documented information, policies or procedures?*
(n=those who have policies and procedures in place related to governance and risk assessment)



Q: *For which of the following do you have documented policies and procedures? Please select all that apply. (n=those who have documented information for the protection of client records and information)*

External cybersecurity threats	76%
Internal vulnerabilities	73%
Potential business and compliance consequences	71%
Remediation efforts (if applicable)	35%
I don't know	7%
None of the above	1%

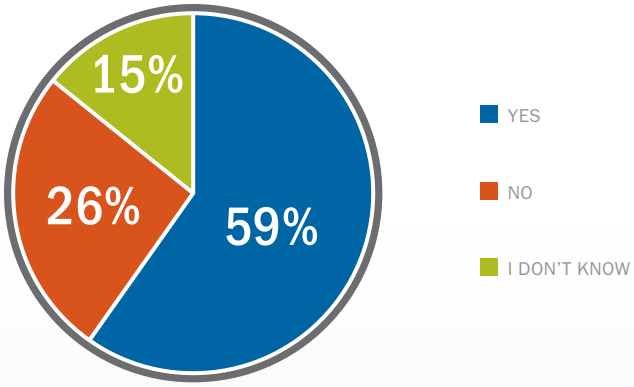
Q: *Which of the following are included in your information regarding periodic risk assessments? (n= those who have documented information for periodic risk assessments).*

	WORKING ON THIS NOW	NOT WORKING ON THIS BUT PLAN TO ADDRESS IT	WE DON'T PLAN TO ADDRESS THIS
Protection of client records and information	71%	18%	12%
Patch management practices	27%	49%	24%
Chief Information Security Officer or other employees responsible for cybersecurity matters	41%	33%	26%
Firm's organizational structure	39%	32%	29%
Periodic risk assessments	38%	40%	22%
Penetration testing including remediation efforts	25%	46%	29%
Vulnerability scans and any remediation efforts	33%	46%	22%

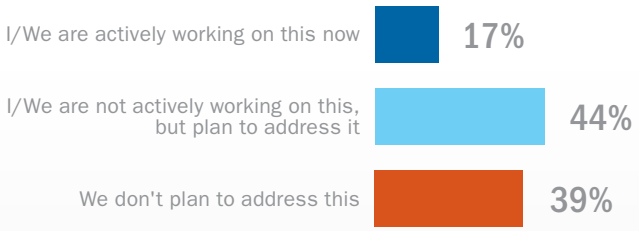
Q: *What are your plans related to documenting policies and procedures for each of the following? (n=those who indicated they did not have policies and procedures in place for these items)*

Access Rights and Controls

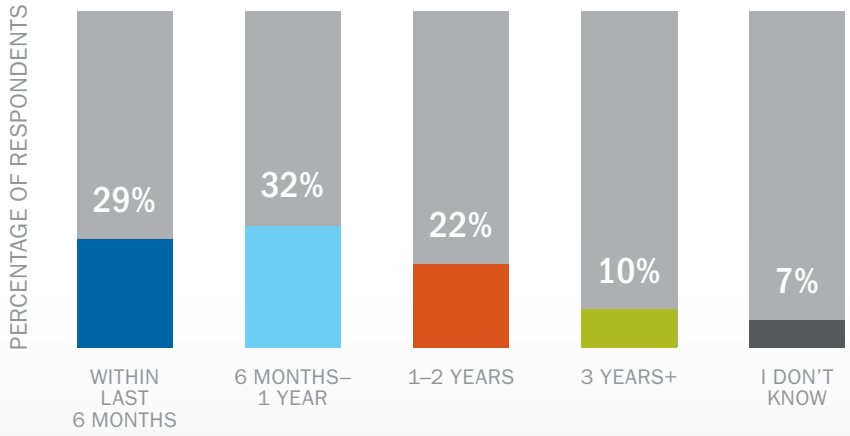
Nearly 60 percent of respondents indicated they had formally documented policies and procedures related to access rights and controls. Respondents were asked detailed questions on exactly how they are preparing across a range of issues associated with this overall category.



Q: *Do you have policies and procedures formally documented today as it relates to access rights and controls (i.e. do associates have access to only what they need to do their job or do they have access to everything)?*



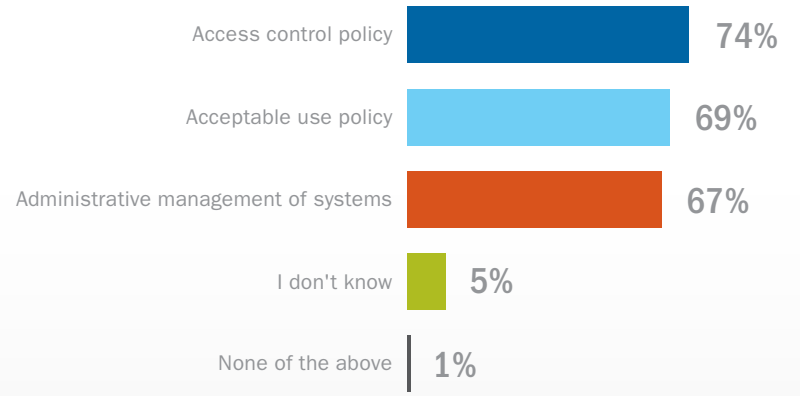
Q: *What are your plans related to documenting policies and procedures for access rights and controls? (n=those who do not have policies and procedures in place related to access rights and controls)*



Q: *When was the bulk of that work completed?*
(n=those who have policies and procedures in place related to access rights and controls)

Verification of the authenticity of customer requests to transfer funds	67%
Employee access rights and controls	63%
A corporate information security policy	56%
System applications and related login security protocols	53%
Devices used to access the firm's system externally	50%
Encryption of devices used to access systems, including ability to remotely monitor, track and deactivate devices	45%
Prevention/identification of unauthorized parties gaining access to network, resources or devices	42%
Reviews of employee access rights/restrictions regarding job-specific resources within the network	42%
Log-in attempts, log-in failures, lockouts and unlocks or resets for perimeter-facing systems	41%
Customer complaints received by the firm related to customer access	41%
Internal audits conducted by the firm regarding access rights and controls	33%
System notifications to users (employees and customers) of appropriate usage obligations when logging into the firm's system (e.g., log-on banners, warning messages or acceptable use notifications)	27%
Instances of anyone receiving access to firm data/systems without authorization	26%
I don't know	11%
None of the above	2%

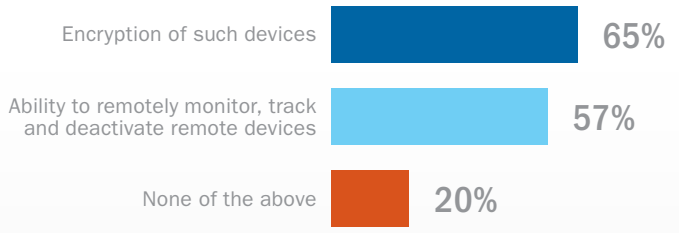
Q: *For which of the following do you have formally documented information, policies or procedures?*
(n=those who have policies and procedures in place related to access rights and controls.)



Q: *Which of the following are included in your information regarding unauthorized access?*
(n=those who have documented information for unauthorized access)

Updating or terminating access rights based on personnel or system changes	57%
Former employees' date their access to the firm's systems was terminated	50%
Former employees' last date of employment	49%
Employee access rights, including the employee's role or group membership	44%
Changes to access rights	40%
Manager approvals for those changes	37%
Any management approval required for changes to access rights or controls	35%
Evidence of tracking of employee access rights	27%
Date access for reassigned employees was modified	21%
Date of reassignment of current employees to a new group or function	20%
I don't know	14%
None of the above	9%

Q: *Which of the following are included in your corporate information security policy?*
(n=those who have a corporate information security policy)



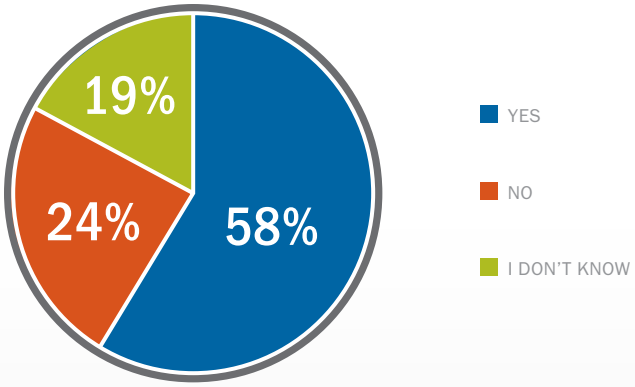
Q: *Do your firm policies regarding devices used to access the firm's system externally include information on the following? (n=those who have policies regarding devices used to access the firm's system externally)*

	WORKING ON THIS NOW	NOT WORKING ON THIS BUT PLAN TO ADDRESS IT	WE DON'T PLAN TO ADDRESS THIS
Prevention/identification of unauthorized parties gaining access to network, resources or devices	37%	46%	17%
A corporate information security policy	39%	41%	20%
Employee access rights and controls	32%	41%	27%
System applications and related login security protocols	39%	36%	25%
Log-in attempts, log-in failures, lockouts and unlocks or resets for perimeter-facing systems	26%	43%	31%
Instances of anyone receiving access to firm data/systems without authorization	34%	46%	20%
System notifications to users (employees and customers) of appropriate usage obligations when logging into the firm's system	23%	44%	33%
Devices used to access the firm's system externally	33%	41%	26%
Encryption of devices used to access systems, including ability to remotely monitor, track and deactivate devices	33%	45%	22%
Customer complaints received by the firm related to customer access	25%	40%	35%
Verification of the authenticity of customer requests to transfer funds	56%	22%	22%
Reviews of employee access rights/restrictions regarding job-specific resources within the network	33%	40%	27%
Internal audits conducted by the firm regarding access rights and controls	27%	47%	25%

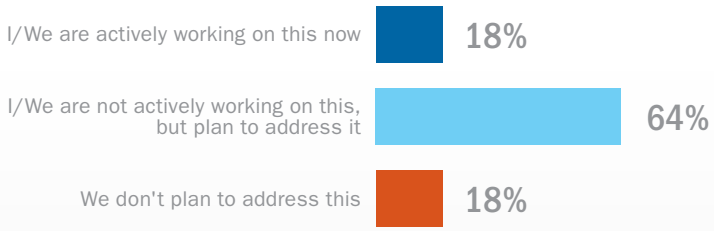
Q: *What are your plans related to documenting policies and procedures for each of the following? (n=those who indicated they did not have policies and procedures in place for these items)*

Data Loss Prevention

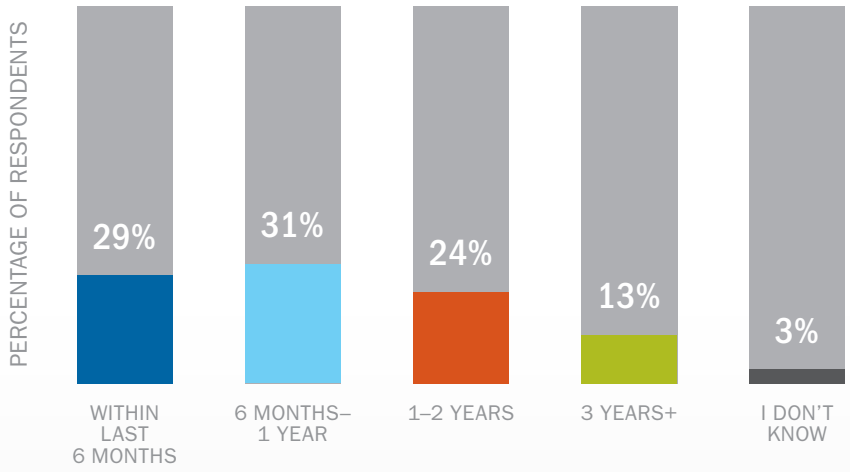
Nearly 60 percent of respondents indicated they had formally documented policies and procedures related to data loss prevention. Respondents were asked detailed questions on exactly how they are preparing across a range of issues associated with this overall category.



Q: *Do you have policies and procedures formally documented today as it relates to data loss prevention?*



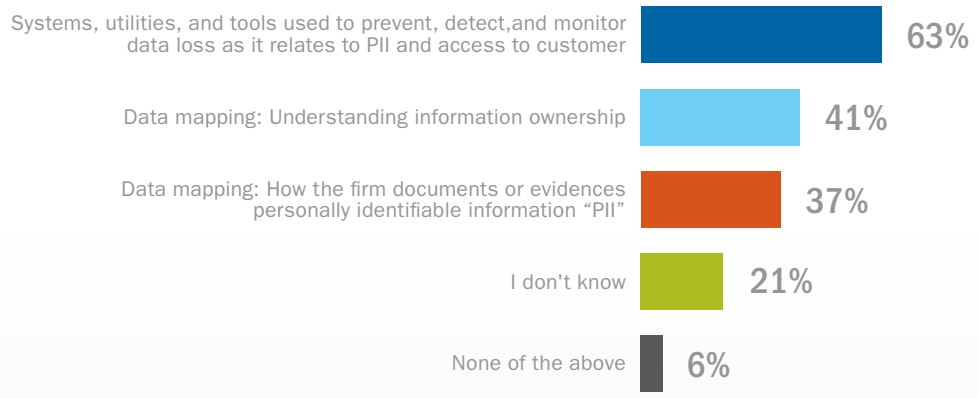
Q: *What are your plans related to documenting policies and procedures for data loss prevention? (n=those who do not have policies and procedures in place related to data loss prevention)*



Q: *When was the bulk of that work completed?*
(n=those who have policies and procedures in place related to data loss prevention)

Policies and procedures related to monitoring unauthorized distribution of sensitive information outside of the firm (e.g. through email, physical media, hard copy)	67%
Policies and procedures related to enterprise data loss prevention and information	65%
I don't know	12%
None of the above	4%

Q: *Which of the following do you have formally documented today as it relates to data loss prevention?*
(n=those who have policies and procedures in place related to data loss prevention)



Q: *Which of the following are included in your policies regarding enterprise data loss prevention? (n=those who have policies and procedures in place related to enterprise data loss prevention)*

Firm policies related to data classification	50%
Risk level associated with each category of data	35%
Factors considered when classifying data	30%
I don't know	25%
None of the above	13%

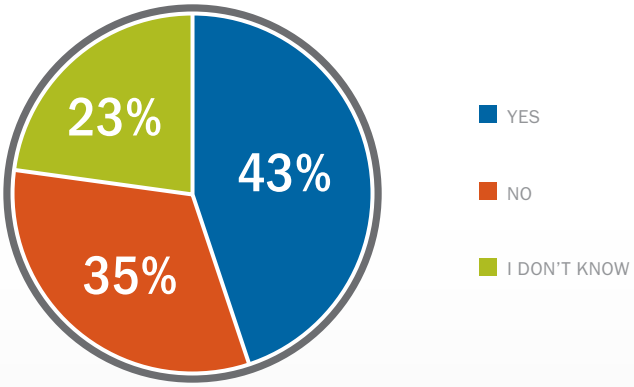
Q: *Which of the following do you have in place related to enterprise data loss prevention? Please select all that apply. (n=those who have policies and procedures in place related to enterprise data loss prevention)*

	WORKING ON THIS NOW	NOT WORKING ON THIS BUT PLAN TO ADDRESS IT	WE DON'T PLAN TO ADDRESS THIS
Policies and procedures related to enterprise data loss prevention and information	15%	65%	20%
Policies and procedures related to monitoring unauthorized distribution of sensitive information outside of the firm	27%	58%	15%

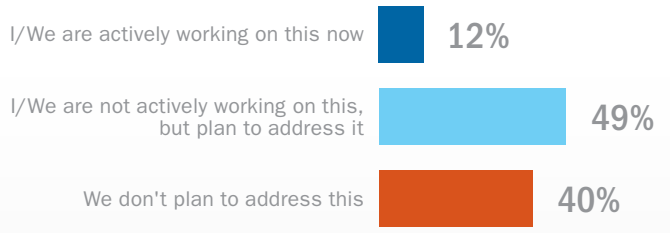
Q: *What are your plans related to documenting policies and procedures for each of the following? (n=those who indicated they did not have policies and procedures in place for these items)*

Vendor Management

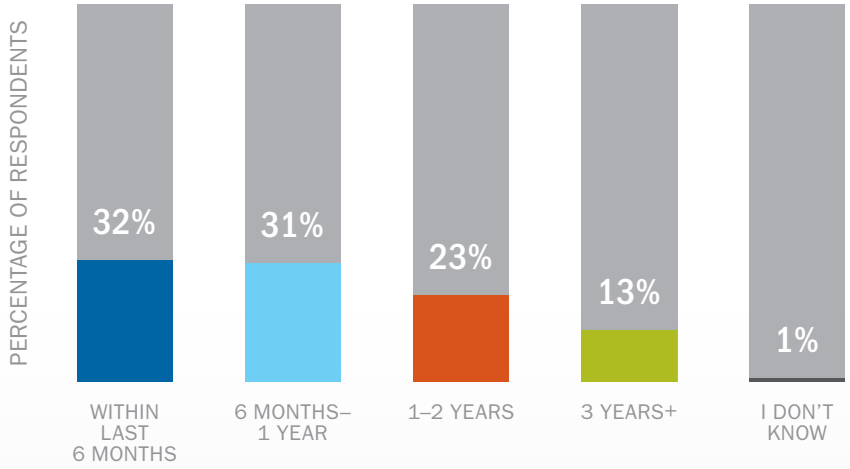
Fewer than half of respondents indicated they had formally documented policies and procedures related to vendor management. Respondents were asked detailed questions on exactly how they are preparing across a range of issues associated with this overall category.



Q: *Do you have policies and procedures formally documented today as it relates to vendor management?*



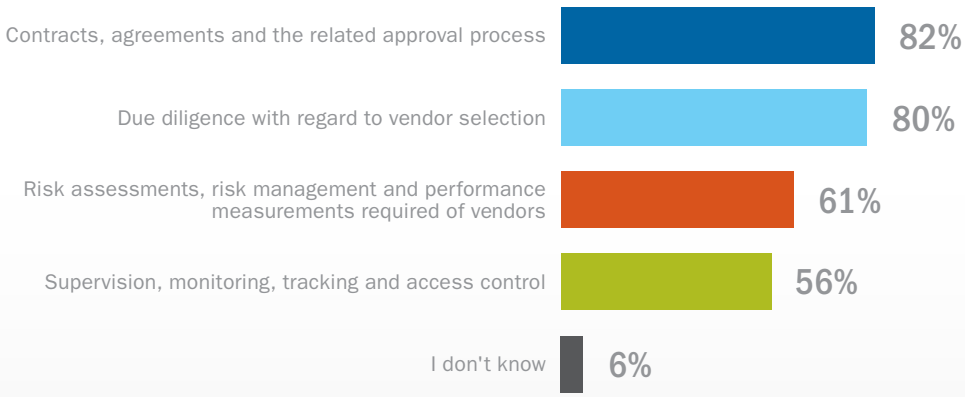
Q: *What are your plans related to documenting policies and procedures for vendor management?*
(n=those who do not have policies and procedures in place related to vendor management)



Q: *When was the bulk of that work completed?*
(n=those who have policies and procedures in place related to vendor management)

Vendors with access to the firm's network or data	70%
Third-party vendors	68%
Third-party vendors that facilitate the mitigation of cybersecurity risks	46%
Sample documents or notices required of third-party vendors	39%
Contingency plans for vendors	35%
I don't know	4%
None of the above	3%

Q: *Which of the following do you have formally documented information, policies or procedures? (n=those who have policies and procedures in place related to vendor management)*



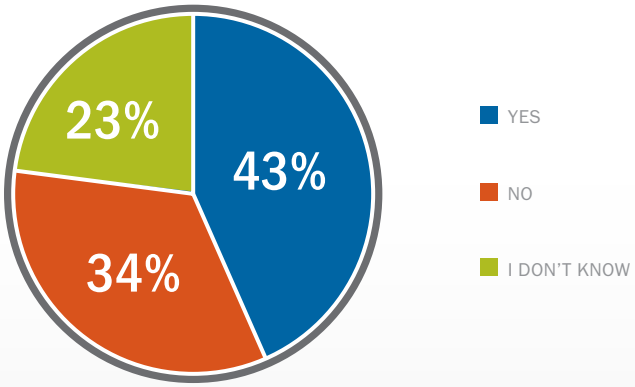
Q: *Which of the following are included in your policies related to third-party vendors? (n=those who have policies and procedures in place related to third party vendors)*

	WORKING ON THIS NOW	NOT WORKING ON THIS BUT PLAN TO ADDRESS IT	WE DON'T PLAN TO ADDRESS THIS
Third-party vendors	33%	47%	21%
Vendors with access to the firm's network or data	29%	32%	39%
Third-party vendors that facilitate the mitigation of cybersecurity risks	34%	38%	28%
Contingency plans for vendors	25%	45%	30%
Sample documents or notices required of third-party vendors	26%	44%	30%

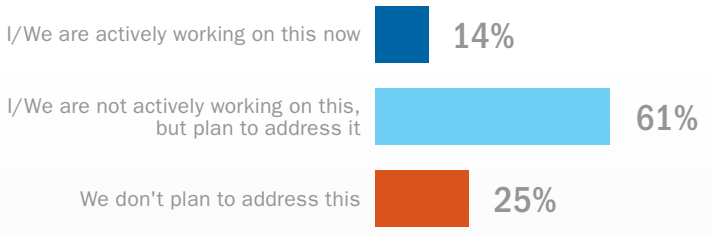
Q: *What are your plans related to documenting policies and procedures for each of the following? (n=those who indicated they did not have policies and procedures in place for these items)*

Incident Response

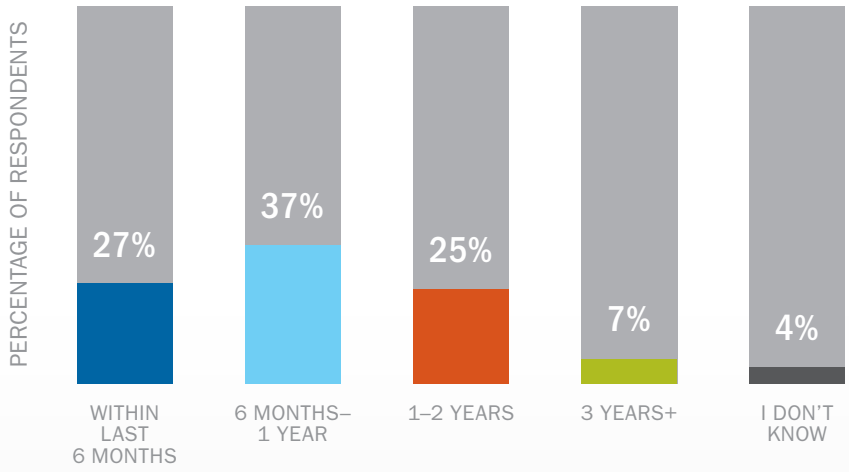
Fewer than half of respondents indicated they had formally documented policies and procedures related to incident response. Respondents were asked detailed questions on exactly how they are preparing across a range of issues associated with this overall category.



Q: *Do you have policies and procedures formally documented today as it relates to incident response?*



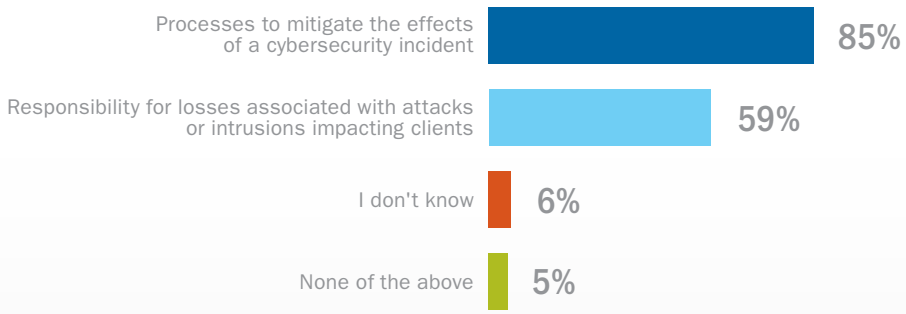
Q: *What are your plans related to documenting policies and procedures for incident response?*
(n=those who do not have policies and procedures in place related to incident response)



Q: *When was the bulk of that work completed?*
(n=those who have policies and procedures in place related to incident response)

Business continuity plan in case of cybersecurity incident	75%
Incidents of unauthorized internal or external distributions of PII	36%
Actual customer losses associated with cyber incidents	36%
Process to test incident response plan	29%
System-generated alerts related to data loss of sensitive/confidential information	28%
Successful unauthorized internal or external incidents related to access	28%
I don't know	11%
None of the above	4%

Q: *Which of the following do you have formally documented today as it relates to incident response?*
(n=those who have policies and procedures in place related to incident response)



Q: *Which of the following are included in your policies related to business continuity and incident reporting?*
(n=those who have policies and procedures in place related to business continuity in case of cybersecurity incident)

Whether the firm had cybersecurity insurance coverage, including the types of incidents the insurance covered	63%
Whether any insurance claims related to cyber events were filed	47%
Amount of cyber-related losses recovered pursuant to the firm's cybersecurity insurance coverage	47%
Amount of customer losses reimbursed by the firm	39%
I don't know	19%
None of the above	10%

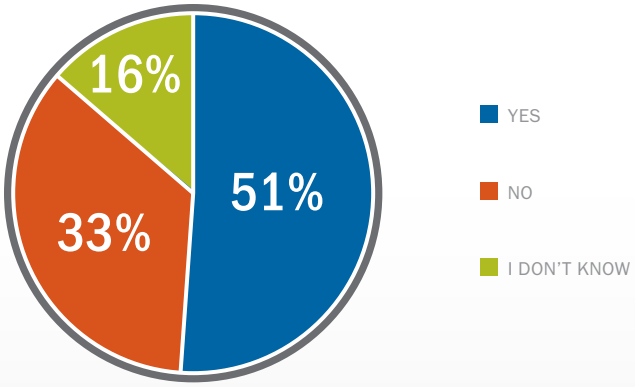
Q: *Which of the following do you have in place related to customer losses associated with cyber incidents? (n=those who have policies and procedures in place related to customer losses)*

	WORKING ON THIS NOW	NOT WORKING ON THIS BUT PLAN TO ADDRESS IT	WE DON'T PLAN TO ADDRESS THIS
Business continuity plan in case of cybersecurity incident	40%	60%	0%
Process to test incident response plan	22%	52%	26%
System-generated alerts related to data loss of sensitive/ confidential information	19%	47%	34%
Incidents of unauthorized internal or external distributions of PII	30%	49%	21%
Successful unauthorized internal or external incidents related to access	29%	54%	17%
Actual customer losses associated with cyber incidents	25%	53%	22%

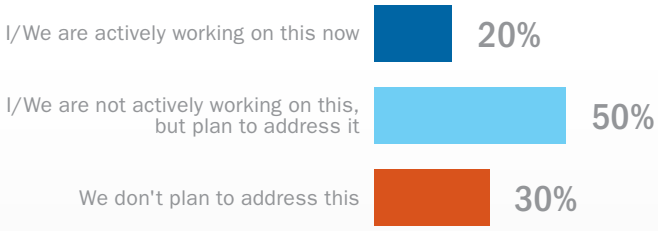
Q: *What are your plans related to documenting policies and procedures for each of the following? n=those who indicated they did not have policies and procedures in place for these items)*

Training

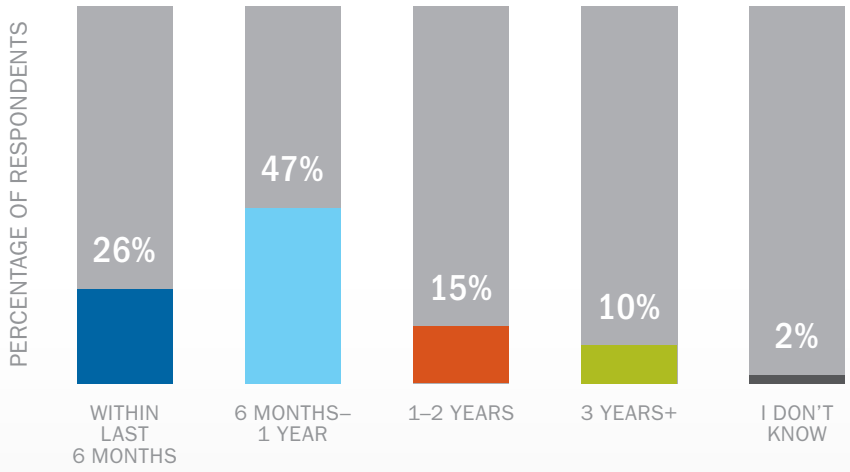
About half of respondents indicated they had formally documented policies and procedures related to employee and vendor training. Respondents (who have teams) were asked detailed questions on exactly how they are preparing across a range of issues associated with this overall category.



Q: *Do you provide employee or vendor training regarding information security and risks?*



Q: *What are your plans related to documenting policies and procedures for employee training? (n=those who do not provide training)*



Q: *When was the bulk of that work completed? (n=those who provide training)*

Training provided to your team regarding information security and risks	**79%**
Training provided to third-party vendors or business partners related to information security	**13%**
I don't know	**12%**
None of the above	**6%**

Q: *Which of the following do you have formally documented today? (n=those who provide training)*

	WORKING ON THIS NOW	NOT WORKING ON THIS BUT PLAN TO ADDRESS IT	WE DON'T PLAN TO ADDRESS THIS
Training provided to your team regarding information security and risks	21%	64%	14%
Training provided to third-party vendors or business partners related to information security.	10%	36%	55%

Q: *What are your plans related to documenting policies and procedures for each of the following? n=those who indicated they did not have policies and procedures in place for these items)*

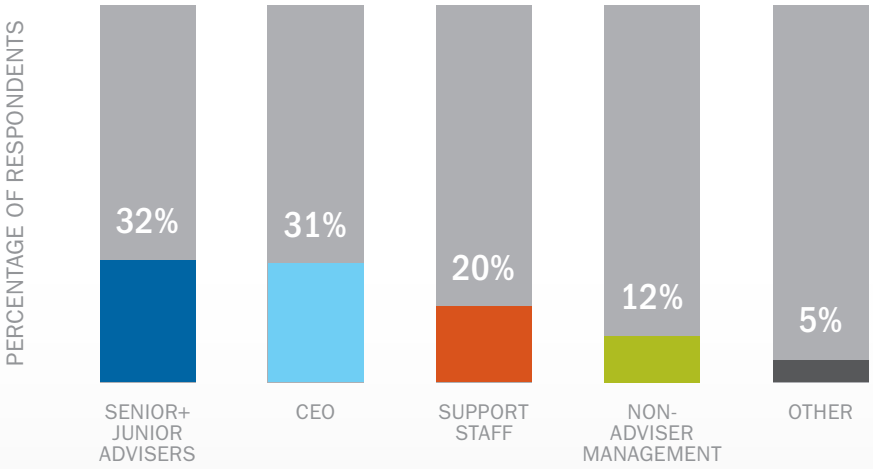
Next Steps

This report focused on the specifics of perception, readiness and execution sharing only the quantitative results. Firms can use this information to assess if they are fully prepared and to compare themselves to their peers.

Going forward, we'll focus on what advisers can do to take meaningful action. Watch for the three upcoming whitepapers that examine client communication, team training and technology best practices

Appendix 1 – Participant Profile

The following is an overview of the 1,015 participants in this study.



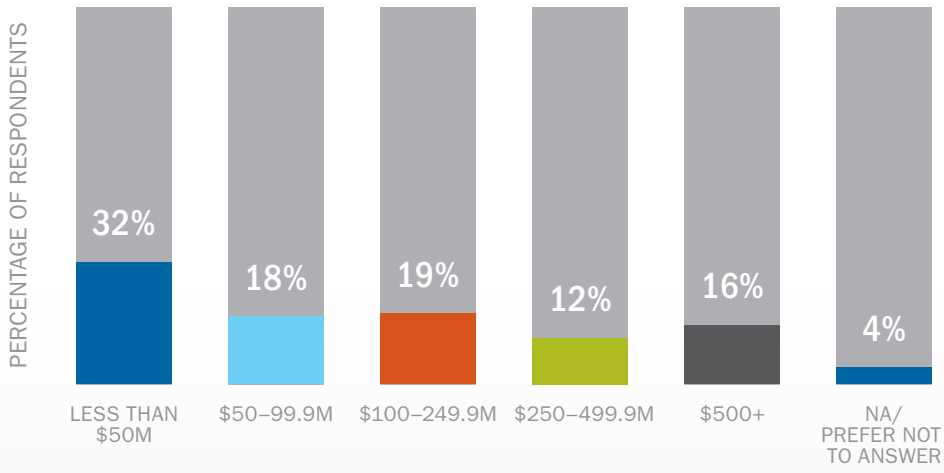
Q: *Which of the following best describes your role?*

Operations	39%
Client Service	26%
Compliance	20%
Finance/Accounting	6%
Other	6%
Marketing	2%
Business Development	2%

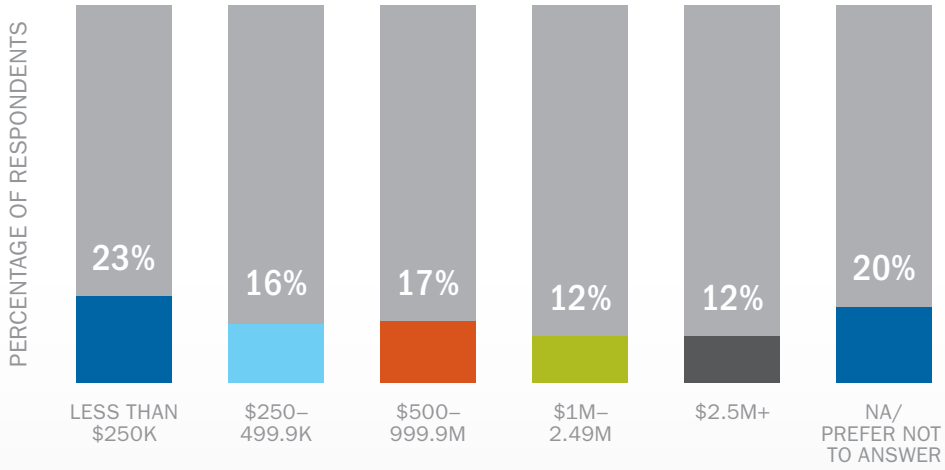
Q: *What is your functional role? Please select one.*

Independent RIA	80%
Hybrid RIA/broker-dealer	9%
National, regional or independent broker-dealer	3%
Other	2%
CPA	1%
Insurance brokerage/agency	1%
National or regional wirehouse	1%
Non-registered fee-only planner	1%
None of the above	1%

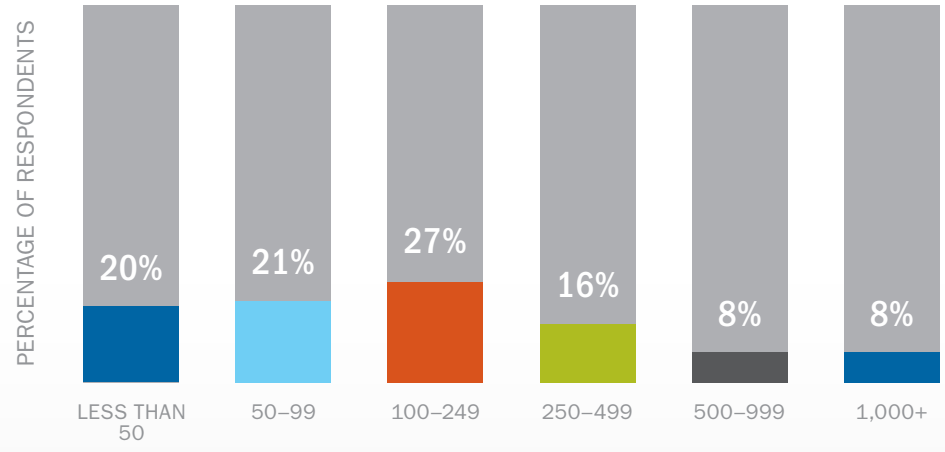
Q: *Which of the following best describes your business model/firm? Please select one.*



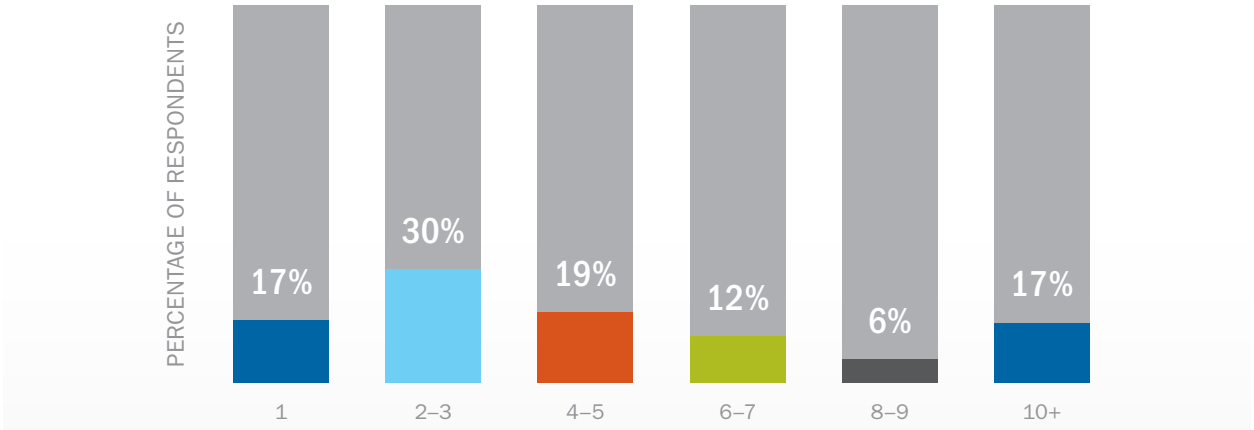
Q: *What are your assets under management today?*



Q: *What was your gross revenue in the last 12 months?*



Q: *With how many client households do you work?*



Q: *Including yourself, how many people are on your team?*

Appendix 2 — Detailed Results by Segment

PERCEPTION AND READINESS

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
How would you describe where cybersecurity ranks amongst your firm's priorities?																			
Very high	29%	28%	25%	39%	35%	27%	27%	23%	34%	40%	26%	32%	26%	25%	27%	24%	30%	27%	37%
High	52%	52%	54%	50%	48%	51%	51%	61%	56%	46%	49%	50%	54%	64%	62%	49%	52%	55%	50%
Neutral	15%	16%	15%	10%	14%	17%	19%	13%	9%	11%	18%	15%	19%	11%	9%	18%	15%	16%	11%
Low	3%	3%	5%	1%	3%	4%	3%	3%	1%	3%	5%	2%	2%	0%	3%	5%	4%	2%	2%
Very low	1%	1%	1%	0%	0%	2%	1%	0%	0%	0%	2%	1%	0%	0%	0%	4%	0%	0%	0%
To what extent would you agree or disagree with the following statements?																			
I fully understand the issues and risks associated with cybersecurity.																			
Completely agree	44%	36%	40%	54%	56%	38%	38%	39%	56%	62%	39%	36%	40%	41%	55%	37%	42%	42%	56%
Somewhat agree	39%	42%	41%	38%	34%	40%	43%	46%	40%	28%	38%	47%	41%	49%	33%	37%	41%	42%	35%
Neutral	6%	8%	7%	4%	7%	9%	6%	5%	2%	5%	10%	5%	8%	4%	3%	12%	6%	5%	5%
Somewhat disagree	8%	12%	10%	4%	2%	10%	11%	9%	3%	5%	9%	11%	11%	4%	9%	11%	9%	9%	3%
Completely disagree	2%	3%	2%	0%	1%	2%	2%	1%	0%	0%	3%	1%	1%	2%	0%	2%	2%	2%	.5%
I am aware of all requirements required to be in place to adhere to the guidelines set by the Office of Compliance Inspections and Examinations.																			
Completely agree	26%	16%	24%	45%	35%	19%	14%	29%	33%	46%	18%	18%	24%	26%	31%	20%	22%	26%	37%
Somewhat agree	37%	32%	36%	41%	42%	32%	39%	38%	47%	35%	30%	37%	38%	41%	48%	27%	36%	40%	40%
Neutral	17%	20%	19%	8%	14%	19%	21%	18%	10%	12%	19%	19%	20%	19%	10%	20%	17%	18%	13%
Somewhat disagree	15%	24%	16%	5%	7%	22%	20%	12%	8%	4%	23%	19%	15%	12%	8%	23%	18%	13%	8%
Completely disagree	5%	9%	5%	1%	2%	8%	6%	3%	2%	3%	10%	6%	3%	3%	3%	10%	7%	3%	2%
I am fully prepared to manage and mitigate the risks associated with cybersecurity.																			
Completely agree	29%	23%	26%	39%	40%	27%	23%	25%	36%	44%	26%	26%	26%	22%	38%	26%	29%	27%	36%
Somewhat agree	45%	46%	46%	49%	41%	43%	43%	53%	47%	41%	40%	48%	44%	58%	50%	38%	42%	50%	48%
Neutral	13%	14%	13%	9%	13%	14%	14%	12%	11%	11%	14%	13%	15%	12%	8%	15%	15%	11%	11%
Somewhat disagree	10%	15%	12%	3%	4%	13%	17%	8%	5%	3%	15%	11%	14%	6%	3%	18%	10%	10%	4%
Completely disagree	2%	3%	3%	1%	1%	4%	3%	1%	0%	1%	5%	3%	0%	2%	1%	4%	3%	2%	1%
To what extent would you agree or disagree with the following statements?																			
My team is aware of all requirements required to be in place to adhere to the guidelines set by the Office of Compliance Inspections and Examinations.																			
Completely agree	17%	11%	13%	23%	25%	16%	13%	17%	13%	27%	16%	14%	13%	16%	17%	0%	16%	15%	22%
Somewhat agree	35%	34%	37%	38%	37%	32%	35%	37%	41%	37%	33%	33%	31%	35%	48%	0%	33%	37%	37%
Neutral	19%	15%	21%	16%	18%	17%	19%	20%	27%	11%	14%	20%	24%	24%	9%	0%	20%	20%	16%
Somewhat disagree	21%	26%	21%	20%	15%	20%	25%	22%	15%	19%	19%	25%	24%	23%	21%	0%	21%	22%	19%
Completely disagree	8%	13%	8%	4%	4%	14%	9%	5%	4%	6%	17%	9%	9%	3%	5%	0%	11%	7%	6%
My team feels confident that we can manage and mitigate the risks associated with cybersecurity.																			
Completely agree	26%	19%	21%	32%	38%	26%	20%	26%	23%	37%	26%	25%	22%	23%	29%	0%	27%	23%	30%
Somewhat agree	47%	46%	50%	49%	44%	41%	46%	50%	61%	44%	41%	37%	46%	59%	56%	0%	44%	48%	50%
Neutral	16%	19%	17%	16%	13%	18%	20%	15%	13%	13%	18%	22%	21%	13%	12%	0%	16%	18%	16%
Somewhat disagree	8%	12%	9%	3%	5%	12%	9%	7%	3%	5%	10%	13%	8%	5%	3%	0%	11%	8%	4%
Completely disagree	2%	4%	3%	0%	1%	3%	5%	1%	0%	0%	5%	3%	3%	1%	0%	0%	3%	3%	1%

CONTINUED ON NEXT PAGE

PERCEPTION AND READINESS–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
If you were to undergo an OCIE cybersecurity examination today, how confident are you that you would pass?																			
Very confident	18%	12%	15%	33%	23%	13%	12%	17%	21%	34%	14%	10%	13%	19%	27%	13%	13%	16%	29%
Somewhat confident	44%	39%	46%	43%	48%	35%	49%	57%	46%	42%	31%	51%	54%	52%	47%	30%	48%	50%	43%
Neutral	17%	20%	16%	14%	15%	22%	16%	12%	20%	10%	24%	20%	13%	16%	15%	21%	18%	15%	15%
Not very confident	13%	17%	15%	7%	7%	17%	17%	9%	7%	7%	18%	13%	14%	11%	4%	20%	12%	12%	7%
Not at all confident	4%	8%	3%	0%	1%	8%	3%	2%	2%	1%	10%	2%	2%	2%	3%	10%	4%	2%	0%
I don't know	5%	5%	5%	3%	6%	5%	3%	4%	4%	7%	3%	4%	4%	1%	4%	5%	3%	5%	6%
Which elements of creating an overall cybersecurity plan do you consider the most challenging to implement?																			
Governance and Risk Assessment	23%	20%	31%	14%	14%	21%	30%	13%	29%	21%	14%	38%	14%	21%	29%	17%	15%	35%	18%
Access Rights and Controls	9%	10%	11%	14%	0%	4%	13%	16%	14%	3%	5%	4%	19%	11%	10%	17%	9%	5%	11%
Data Loss Prevention	22%	22%	20%	33%	14%	21%	22%	23%	7%	29%	29%	12%	14%	32%	19%	22%	29%	21%	16%
Vendor Management	23%	34%	11%	24%	29%	25%	26%	26%	21%	18%	29%	31%	19%	21%	19%	33%	24%	16%	26%
Incident Response	11%	7%	7%	14%	29%	18%	0%	6%	21%	15%	14%	4%	10%	16%	5%	6%	12%	9%	16%
Training	12%	7%	20%	0%	14%	11%	9%	16%	7%	15%	10%	12%	24%	0%	19%	6%	12%	14%	13%
Do you feel your approach to dealing with cybersecurity risks is a competitive advantage relative to other advisers?																			
Yes	32%	27%	28%	43%	41%	28%	32%	29%	38%	44%	25%	32%	30%	31%	45%	24%	30%	34%	40%
No	39%	46%	44%	31%	25%	42%	40%	43%	35%	30%	45%	44%	40%	40%	38%	44%	45%	35%	30%
I don't know	29%	26%	28%	26%	34%	30%	27%	28%	28%	27%	30%	24%	29%	30%	18%	32%	25%	31%	30%
To what extent do you think your clients are aware of the risks associated with data security?																			
Very aware	11%	10%	9%	10%	14%	9%	7%	11%	15%	12%	10%	6%	8%	10%	15%	11%	9%	10%	14%
Somewhat aware	59%	52%	61%	65%	61%	58%	54%	61%	55%	66%	58%	55%	62%	60%	59%	55%	61%	57%	61%
Neutral	11%	13%	11%	10%	9%	12%	14%	13%	11%	4%	12%	14%	10%	12%	8%	11%	11%	11%	11%
Not very aware	17%	23%	17%	13%	14%	19%	23%	13%	17%	15%	18%	22%	19%	15%	16%	21%	18%	19%	12%
Not at all aware	2%	2%	2%	0%	0%	2%	2%	2%	2%	0%	2%	2%	1%	3%	1%	2%	1%	2%	0%
I don't know	1%	1%	0%	2%	2%	0%	0%	1%	0%	3%	0%	0%	1%	0%	0%	1%	1%	1%	1%

CONTINUED ON NEXT PAGE

PERCEPTION AND READINESS–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
To what extent do you think your clients are worried about security breaches with respect to their data?																			
Very worried	11%	12%	11%	6%	10%	10%	7%	10%	14%	13%	11%	9%	6%	14%	9%	9%	8%	13%	12%
Somewhat worried	52%	49%	56%	58%	45%	49%	55%	56%	52%	52%	51%	51%	52%	51%	51%	53%	51%	49%	57%
Neutral	18%	18%	17%	21%	18%	17%	23%	17%	17%	17%	17%	18%	23%	19%	23%	15%	19%	21%	14%
Not very worried	16%	17%	14%	12%	24%	20%	14%	15%	13%	15%	17%	20%	17%	14%	14%	17%	19%	14%	16%
Not at all worried	1%	2%	1%	1%	0%	1%	1%	0%	2%	1%	1%	1%	1%	0%	1%	2%	1%	0%	0%
I don't know	2%	2%	2%	2%	3%	3%	1%	2%	2%	2%	2%	1%	2%	2%	1%	5%	2%	2%	0%
How much have you spent externally in the last 12 months, in total, in order to define or implement policies and procedures related to cybersecurity?																			
We have not invested externally	23%	36%	22%	10%	12%	42%	23%	12%	10%	5%	48%	25%	16%	10%	5%	51%	28%	15%	4%
Less than $5,000	37%	47%	35%	35%	27%	44%	46%	39%	29%	13%	41%	50%	48%	37%	23%	37%	45%	40%	21%
$5,000–$9,999	12%	9%	15%	16%	8%	6%	13%	17%	21%	13%	4%	13%	12%	23%	28%	4%	10%	14%	19%
$10,000–$14,999	4%	2%	3%	8%	6%	0%	3%	5%	6%	9%	0%	2%	5%	4%	14%	0%	2%	4%	9%
$15,000+	6%	4%	4%	12%	8%	1%	2%	6%	5%	23%	1%	1%	2%	9%	11%	1%	2%	6%	15%
I don't know	19%	3%	23%	19%	39%	7%	14%	22%	28%	37%	5%	9%	16%	17%	19%	8%	13%	22%	32%
How much have you invested in internal resources in the last 12 months, in total, in order to define or implement policies and procedures related to cybersecurity?																			
We have not invested externally	21%	30%	23%	6%	13%	37%	19%	14%	10%	5%	46%	21%	12%	11%	12%	43%	25%	14%	7%
Less than $5,000	44%	57%	41%	46%	30%	52%	57%	44%	37%	19%	46%	61%	61%	42%	30%	46%	53%	47%	26%
$5,000–$9,999	8%	5%	11%	7%	8%	4%	7%	13%	17%	5%	3%	9%	4%	20%	20%	2%	7%	7%	15%
$10,000–$14,999	3%	1%	2%	8%	3%	1%	0%	3%	4%	9%	0%	1%	2%	3%	8%	1%	2%	4%	4%
$15,000+	5%	4%	3%	12%	7%	1%	3%	4%	6%	19%	0%	0%	4%	7%	14%	1%	1%	5%	15%
I don't know	19%	3%	21%	21%	39%	5%	14%	22%	27%	42%	3%	8%	18%	17%	16%	7%	12%	23%	33%
In the last year, how much time have you personally invested in understanding or managing the implementation of policies and procedures related to cybersecurity?																			
Less than 10 hours	37%	39%	43%	23%	34%	47%	39%	31%	30%	27%	51%	38%	34%	26%	31%	52%	41%	30%	30%
10–19 hours	28%	30%	28%	25%	24%	26%	33%	30%	29%	23%	24%	32%	33%	36%	22%	24%	28%	31%	24%
20–29 hours	13%	12%	11%	14%	13%	10%	10%	15%	16%	13%	10%	15%	9%	20%	12%	9%	12%	12%	17%
30–39 hours	4%	4%	4%	9%	4%	4%	2%	7%	5%	3%	5%	3%	5%	3%	7%	2%	4%	5%	5%
40 hours+	13%	11%	7%	27%	15%	9%	11%	11%	13%	25%	7%	9%	13%	12%	22%	8%	10%	14%	18%
I don't know	6%	3%	7%	3%	10%	3%	5%	6%	6%	9%	3%	2%	5%	2%	7%	4%	4%	7%	7%

GOVERNANCE AND RISK

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
Do you feel your approach to dealing with cybersecurity risks is a competitive advantage relative to other advisers?																			
Yes	57%	53%	54%	68%	59%	46%	57%	64%	64%	69%	44%	58%	54%	70%	75%	49%	48%	64%	65%
No	24%	35%	25%	15%	9%	38%	23%	15%	15%	12%	42%	23%	23%	15%	14%	40%	30%	16%	13%
I don't know	19%	12%	21%	17%	32%	16%	20%	21%	20%	18%	14%	19%	23%	16%	11%	11%	22%	20%	22%
What are your plans related to documenting policies and procedures for governance and risk assessment? (if not in place today)																			
I/We are actively working on this now	23%	16%	22%	53%	36%	13%	26%	33%	60%	47%	13%	15%	30%	56%	60%	12%	18%	38%	46%
I/We are not actively working on this, but plan to address it	53%	58%	51%	47%	50%	62%	38%	54%	33%	41%	59%	64%	48%	44%	20%	52%	61%	45%	46%
We don't plan to address this	23%	26%	28%	0%	14%	25%	35%	13%	7%	12%	28%	21%	21%	0%	20%	35%	22%	18%	8%
When was the bulk of that work completed?																			
Within last 6 months	36%	42%	39%	24%	36%	38%	41%	37%	30%	31%	43%	36%	32%	34%	32%	45%	41%	31%	32%
6 months–1 year	35%	31%	33%	47%	30%	27%	32%	41%	39%	42%	18%	28%	49%	45%	43%	19%	33%	36%	47%
1–2 years	18%	20%	19%	20%	15%	21%	17%	20%	15%	18%	20%	26%	15%	18%	14%	21%	14%	23%	14%
3 years+	7%	5%	3%	7%	13%	11%	7%	0%	6%	7%	11%	11%	2%	3%	4%	7%	10%	6%	3%
I don't know	4%	1%	6%	2%	6%	3%	2%	2%	9%	2%	7%	0%	2%	0%	7%	7%	2%	4%	3%
For which of the following do you have formally documented information, policies or procedures?																			
Protection of client records and information	85%	94%	77%	83%	85%	89%	87%	85%	84%	77%	86%	92%	84%	88%	82%	87%	90%	86%	78%
Periodic risk assessments	64%	61%	64%	63%	66%	55%	64%	69%	70%	67%	51%	57%	78%	67%	71%	48%	76%	62%	67%
Firm's organizational structure (specifically positions responsible for cybersecurity-related matters)	59%	52%	56%	63%	68%	50%	58%	65%	57%	65%	43%	71%	51%	69%	64%	37%	54%	70%	65%
Chief Information Security Officer (or equivalent) or other employees responsible for cybersecurity matters	48%	35%	42%	60%	57%	32%	49%	49%	51%	65%	33%	39%	58%	31%	75%	30%	48%	50%	57%
Vulnerability scans and any remediation efforts	37%	32%	40%	38%	32%	32%	33%	36%	35%	50%	27%	33%	40%	33%	61%	33%	43%	32%	41%
Patch management practices (e.g., prompt installation and documentation of critical patches)	34%	31%	29%	50%	30%	25%	18%	44%	32%	50%	22%	27%	27%	38%	50%	22%	33%	37%	39%
Penetration testing (conducted by or on behalf of the firm) including remediation efforts	21%	18%	12%	27%	21%	11%	16%	24%	19%	35%	4%	18%	27%	24%	21%	9%	22%	21%	26%
I don't know	8%	1%	10%	10%	11%	3%	7%	11%	8%	12%	4%	4%	7%	10%	0%	2%	6%	8%	13%
None of the above	1%	3%	1%	0%	0%	4%	0%	0%	0%	0%	6%	0%	0%	0%	0%	7%	0%	0%	0%

CONTINUED ON NEXT PAGE

GOVERNANCE AND RISK–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
For which of the following do you have documented policies and procedures?																			
Security of customer documents and information	93%	94%	89%	95%	96%	94%	92%	91%	90%	97%	95%	96%	92%	78%	100%	98%	92%	93%	92%
Protection against unauthorized access to customer accounts or information	81%	72%	91%	83%	76%	71%	87%	83%	83%	87%	67%	84%	87%	86%	83%	70%	80%	87%	81%
Protection against anticipated threats to customer information	65%	61%	59%	74%	64%	56%	67%	62%	60%	85%	52%	67%	58%	68%	91%	53%	65%	67%	72%
Permitted and prohibited uses for company provided devices in accessing client information	63%	54%	68%	76%	60%	56%	51%	70%	60%	79%	55%	51%	66%	68%	74%	48%	62%	62%	79%
I don't know	1%	3%	0%	0%	0%	3%	0%	0%	0%	0%	2%	2%	0%	0%	0%	0%	3%	0%	0%
None of the above	0%	1%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%	3%	0%	0%	3%	0%	0%	0%
Which of the following are included in your information regarding periodic risk assessment?																			
External cybersecurity threats	76%	80%	65%	88%	71%	60%	86%	82%	77%	76%	60%	68%	88%	86%	70%	60%	75%	78%	82%
Internal vulnerabilities	73%	78%	65%	79%	66%	60%	93%	74%	65%	74%	60%	79%	91%	57%	60%	65%	84%	65%	73%
Potential business and compliance consequences	71%	73%	74%	67%	66%	73%	68%	79%	62%	68%	56%	79%	79%	68%	65%	50%	73%	82%	67%
Remediation efforts (if applicable)	35%	24%	28%	45%	46%	28%	25%	42%	38%	41%	12%	46%	35%	43%	30%	30%	33%	33%	42%
I don't know	7%	4%	11%	3%	11%	8%	0%	3%	12%	15%	12%	4%	0%	7%	20%	10%	2%	5%	13%
None of the above	1%	2%	0%	0%	0%	3%	0%	0%	0%	0%	4%	0%	0%	0%	0%	5%	0%	0%	0%
What are your plans related to documenting policies and procedures for:																			
Protection of client records and information?																			
I/We are actively working on this now	71%	50%	75%	67%	100%	67%	100%	50%	100%	60%	80%	50%	67%	0%	75%	80%	33%	80%	75%
I/We are not actively working on this, but plan to address it	18%	25%	13%	33%	0%	17%	0%	50%	0%	20%	20%	0%	33%	100%	0%	20%	33%	20%	0%
We don't plan to address this	12%	25%	13%	0%	0%	17%	0%	0%	0%	20%	0%	50%	0%	0%	25%	0%	33%	0%	25%
Patch management practices?																			
I/We are actively working on this now	27%	18%	30%	30%	29%	28%	30%	32%	15%	30%	31%	21%	31%	27%	15%	30%	41%	13%	28%
I/We are not actively working on this, but plan to address it	49%	42%	51%	50%	58%	42%	42%	48%	65%	60%	39%	48%	45%	64%	62%	30%	37%	65%	59%
We don't plan to address this	24%	40%	19%	20%	13%	30%	27%	20%	20%	10%	31%	30%	24%	9%	23%	39%	22%	23%	13%

CONTINUED ON NEXT PAGE

GOVERNANCE AND RISK–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
What are your plans related to documenting policies and procedures for: –CONTINUED																			
Chief Information Security Officer or other employees responsible for cybersecurity matters?																			
I/We are actively working on this now	41%	24%	50%	64%	41%	26%	42%	64%	57%	36%	19%	41%	53%	44%	43%	21%	45%	50%	45%
I/We are not actively working on this, but plan to address it	33%	37%	29%	21%	41%	43%	26%	27%	21%	36%	42%	41%	13%	36%	29%	32%	42%	25%	35%
We don't plan to address this	26%	39%	21%	14%	18%	32%	32%	9%	21%	27%	39%	19%	33%	20%	29%	46%	13%	25%	20%
Firm's organizational structure?																			
I/We are actively working on this now	39%	24%	35%	62%	45%	27%	47%	31%	58%	55%	27%	36%	39%	33%	67%	36%	37%	37%	54%
I/We are not actively working on this, but plan to address it	32%	30%	39%	31%	36%	33%	40%	31%	25%	27%	31%	45%	39%	22%	11%	20%	44%	37%	23%
We don't plan to address this	29%	45%	26%	8%	18%	39%	13%	38%	17%	18%	42%	18%	22%	44%	22%	44%	19%	26%	23%
Periodic risk assessments?																			
I/We are actively working on this now	38%	18%	44%	75%	25%	32%	31%	45%	17%	70%	36%	22%	29%	50%	71%	36%	17%	38%	58%
I/We are not actively working on this, but plan to address it	40%	50%	33%	8%	67%	42%	46%	36%	50%	20%	45%	44%	57%	30%	14%	36%	58%	42%	25%
We don't plan to address this	22%	32%	22%	17%	8%	26%	23%	18%	33%	10%	18%	33%	14%	20%	14%	27%	25%	19%	17%
Penetration testing including remediation efforts?																			
I/We are actively working on this now	25%	13%	22%	39%	39%	20%	26%	25%	28%	33%	27%	22%	28%	18%	29%	23%	27%	24%	28%
I/We are not actively working on this, but plan to address it	46%	43%	53%	42%	44%	42%	44%	44%	56%	52%	38%	41%	48%	57%	52%	31%	42%	55%	53%
We don't plan to address this	29%	43%	25%	19%	17%	38%	29%	31%	16%	15%	36%	38%	24%	25%	19%	46%	31%	21%	20%
Vulnerability scans and any remediation efforts?																			
I/We are actively working on this now	33%	18%	34%	36%	47%	23%	35%	31%	53%	32%	29%	17%	48%	29%	30%	32%	32%	35%	30%
I/We are not actively working on this, but plan to address it	46%	45%	51%	56%	40%	40%	42%	66%	37%	53%	32%	57%	43%	63%	40%	21%	44%	58%	50%
We don't plan to address this	22%	37%	14%	8%	13%	38%	23%	3%	11%	16%	38%	27%	9%	8%	30%	46%	24%	8%	20%

ACCESS RIGHTS AND CONTROLS

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
Do you have policies and procedures formally documented today as it relates to access rights and controls?																			
Yes	59%	56%	60%	71%	55%	54%	62%	60%	65%	66%	53%	64%	56%	69%	66%	55%	60%	63%	58%
No	26%	35%	25%	18%	19%	35%	30%	22%	20%	16%	36%	28%	32%	17%	23%	35%	28%	24%	20%
I don't know	15%	9%	15%	11%	26%	11%	8%	18%	15%	18%	11%	9%	12%	14%	11%	10%	12%	13%	23%
What are your plans related to documenting policies and procedures for access rights and controls? (if not in place today)																			
I/We are actively working on this now	17%	13%	13%	35%	24%	11%	2%	21%	37%	48%	9%	10%	18%	17%	63%	5%	16%	14%	39%
I/We are not actively working on this, but plan to address it	44%	42%	46%	41%	48%	39%	60%	44%	42%	38%	37%	56%	50%	39%	25%	35%	50%	50%	37%
We don't plan to address this	39%	46%	41%	24%	28%	49%	37%	35%	21%	14%	53%	33%	32%	44%	13%	60%	34%	36%	24%
When was the bulk of that work completed?																			
Within last 6 months	29%	35%	26%	22%	31%	32%	33%	34%	23%	15%	40%	29%	29%	26%	10%	26%	41%	25%	20%
6 months–1 year	32%	31%	29%	40%	27%	21%	36%	30%	35%	45%	19%	24%	42%	32%	45%	29%	23%	36%	43%
1–2 years	22%	24%	22%	24%	18%	26%	17%	27%	26%	15%	26%	24%	16%	32%	20%	31%	23%	22%	16%
3 years+	10%	8%	14%	7%	11%	14%	11%	2%	6%	15%	13%	11%	11%	3%	15%	9%	11%	10%	10%
I don't know	7%	2%	9%	7%	13%	7%	3%	7%	10%	10%	2%	11%	3%	8%	10%	6%	3%	8%	12%
For which of the following do you have formally documented information, policies or procedures?																			
Verification of the authenticity of customer requests to transfer funds	67%	63%	56%	84%	69%	65%	62%	67%	72%	70%	59%	68%	64%	72%	65%	60%	65%	68%	72%
Employee access rights and controls	63%	55%	55%	76%	73%	55%	55%	65%	67%	74%	46%	70%	64%	64%	65%	44%	62%	64%	76%
A corporate information security policy	56%	43%	53%	67%	71%	48%	57%	63%	64%	57%	47%	55%	64%	44%	52%	40%	60%	62%	57%
System applications and related login security protocols	53%	45%	37%	69%	65%	42%	48%	59%	67%	57%	31%	57%	62%	49%	65%	42%	48%	60%	59%
Encryption of devices used to access systems, including ability to remotely monitor, track and deactivate devices	45%	42%	36%	51%	55%	42%	38%	39%	50%	59%	36%	43%	38%	46%	39%	42%	35%	53%	50%
Reviews of employee access rights/ restrictions regarding job-specific resources within the network	42%	41%	33%	47%	53%	36%	31%	47%	36%	59%	32%	47%	42%	46%	39%	33%	40%	48%	43%
Log-in attempts, log-in failures, lockouts and unlocks or resets for perimeter-facing systems	41%	32%	40%	57%	43%	40%	31%	37%	42%	52%	37%	45%	33%	41%	43%	35%	39%	43%	45%
Customer complaints received by the firm related to customer access	41%	38%	36%	49%	45%	40%	29%	43%	39%	48%	36%	45%	31%	36%	43%	33%	35%	48%	43%
Internal audits conducted by the firm regarding access rights and controls	33%	24%	25%	45%	41%	23%	26%	29%	33%	54%	22%	34%	29%	44%	35%	23%	24%	37%	45%
I don't know	11%	13%	12%	6%	8%	12%	10%	8%	11%	13%	17%	2%	11%	3%	13%	14%	10%	9%	12%
None of the above	2%	4%	1%	2%	0%	2%	2%	2%	3%	0%	3%	2%	2%	0%	0%	5%	2%	1%	0%

CONTINUED ON NEXT PAGE

ACCESS RIGHTS AND CONTROLS–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
Which of the following are included in your information regarding unauthorized access?																			
Access control policy	74%	78%	81%	77%	55%	77%	64%	77%	76%	67%	88%	77%	59%	69%	86%	85%	69%	81%	67%
Acceptable use policy	69%	81%	70%	73%	35%	71%	86%	69%	53%	67%	65%	86%	88%	56%	71%	69%	69%	75%	60%
Administrative management of systems	67%	59%	70%	67%	70%	66%	71%	46%	71%	67%	59%	77%	76%	63%	57%	46%	72%	75%	60%
I don't know	5%	4%	4%	3%	10%	6%	0%	0%	6%	8%	6%	5%	0%	0%	0%	15%	3%	3%	3%
None of the above	1%	0%	0%	0%	5%	0%	0%	8%	0%	0%	0%	0%	6%	0%	0%	0%	0%	3%	0%
Which of the following are included in your corporate information security policy information regarding unauthorized access?																			
Updating or terminating access rights based on personnel or system changes	57%	52%	50%	77%	52%	43%	50%	70%	50%	68%	37%	52%	69%	40%	75%	47%	52%	61%	63%
Former employees' date their access to the firm's systems was terminated	50%	52%	39%	68%	42%	46%	20%	63%	55%	56%	41%	43%	69%	33%	58%	59%	43%	54%	50%
Former employees' last date of employment	49%	38%	47%	74%	39%	43%	35%	60%	45%	56%	44%	39%	65%	33%	58%	47%	43%	50%	56%
Employee access rights, including the employee's role or group membership	44%	41%	39%	61%	39%	43%	35%	37%	36%	60%	33%	48%	46%	20%	58%	29%	43%	48%	47%
Changes to access rights	40%	38%	39%	52%	30%	41%	40%	33%	23%	52%	41%	39%	35%	20%	33%	41%	34%	41%	44%
Manager approvals for those changes	37%	52%	26%	45%	27%	38%	25%	33%	32%	52%	37%	35%	42%	7%	42%	41%	27%	46%	38%
Any management approval required for changes to access rights or controls	35%	38%	26%	35%	33%	30%	35%	27%	32%	48%	26%	43%	42%	7%	33%	29%	34%	41%	28%
Evidence of tracking of employee access rights	27%	31%	21%	42%	21%	30%	15%	13%	14%	52%	33%	26%	15%	7%	33%	29%	25%	24%	34%
Date access for reassigned employees was modified	21%	24%	11%	35%	18%	22%	15%	13%	5%	44%	19%	17%	27%	0%	25%	35%	16%	17%	25%
Date of reassignment of current employees to a new group or function	20%	21%	18%	26%	18%	22%	15%	7%	18%	36%	22%	17%	19%	0%	17%	41%	14%	17%	22%
I don't know	14%	14%	13%	3%	27%	11%	5%	7%	27%	24%	11%	9%	0%	33%	8%	6%	7%	17%	22%
None of the above	9%	14%	8%	10%	6%	14%	20%	3%	5%	4%	22%	9%	4%	13%	8%	29%	14%	0%	6%
Do your firm policies regarding devices used to access the firms system externally including information on...?																			
Encryption of such devices	65%	76%	56%	65%	67%	65%	60%	59%	63%	72%	70%	52%	62%	59%	57%	73%	63%	70%	58%
Ability to remotely monitor, track, and deactivate remote devices	57%	45%	63%	69%	58%	62%	27%	59%	56%	66%	57%	52%	33%	65%	71%	60%	46%	58%	67%
None of the above	20%	21%	19%	15%	21%	16%	40%	23%	25%	10%	17%	24%	33%	29%	14%	20%	23%	20%	18%

CONTINUED ON NEXT PAGE

ACCESS RIGHTS AND CONTROLS–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
What are your plans related to documenting procedures for:																			
Prevention/identification of unauthorized parties gaining access to network, resources or devices.																			
I/We are actively working on this now	37%	38%	34%	38%	41%	31%	35%	48%	50%	25%	41%	21%	38%	53%	23%	24%	44%	39%	29%
I/We are not actively working on this, but plan to address it	46%	35%	51%	46%	45%	47%	53%	41%	25%	56%	34%	68%	57%	41%	54%	38%	46%	55%	41%
We don't plan to address this	17%	26%	14%	15%	14%	22%	12%	10%	25%	19%	24%	11%	5%	6%	23%	38%	10%	6%	29%
A corporate information security policy.																			
I/We are actively working on this now	39%	55%	25%	40%	30%	44%	64%	43%	13%	23%	47%	35%	45%	40%	38%	29%	44%	50%	25%
I/We are not actively working on this, but plan to address it	41%	23%	54%	40%	50%	34%	36%	29%	50%	62%	32%	47%	36%	40%	63%	41%	40%	32%	56%
We don't plan to address this	20%	23%	21%	20%	20%	22%	0%	29%	38%	15%	21%	18%	18%	20%	0%	29%	16%	18%	19%
Employee access rights and controls.																			
I/We are actively working on this now	32%	19%	35%	38%	38%	22%	45%	42%	43%	17%	24%	40%	50%	45%	20%	35%	14%	45%	40%
I/We are not actively working on this, but plan to address it	41%	48%	48%	25%	25%	41%	36%	33%	29%	83%	33%	50%	50%	36%	60%	12%	62%	45%	40%
We don't plan to address this	27%	33%	17%	38%	38%	37%	18%	25%	29%	0%	43%	10%	0%	18%	20%	53%	24%	10%	20%
System applications and related login security protocols.																			
I/We are actively working on this now	39%	36%	36%	33%	58%	33%	54%	47%	20%	38%	29%	47%	50%	50%	20%	35%	34%	41%	50%
I/We are not actively working on this, but plan to address it	36%	36%	39%	44%	17%	39%	23%	27%	60%	38%	39%	29%	30%	43%	40%	24%	41%	45%	25%
We don't plan to address this	25%	29%	24%	22%	25%	28%	23%	27%	20%	23%	32%	24%	20%	7%	40%	41%	25%	14%	25%
Log-in attempts, log-in failures, lockouts and unlocks or resets for perimeter-facing systems.																			
I/We are actively working on this now	26%	22%	26%	31%	30%	24%	42%	25%	15%	20%	27%	25%	26%	31%	20%	19%	30%	28%	24%
I/We are not actively working on this, but plan to address it	43%	43%	41%	38%	45%	35%	26%	46%	62%	60%	38%	35%	52%	56%	50%	33%	35%	56%	48%
We don't plan to address this	31%	35%	32%	31%	25%	41%	32%	29%	23%	20%	35%	40%	22%	13%	30%	48%	35%	16%	29%
Instances of anyone receiving access to firm data/systems without authorization.																			
I/We are actively working on this now	34%	27%	35%	30%	48%	26%	54%	41%	30%	21%	30%	38%	47%	19%	19%	20%	38%	40%	31%
I/We are not actively working on this, but plan to address it	46%	43%	47%	55%	32%	43%	38%	35%	55%	63%	36%	50%	44%	62%	63%	40%	42%	49%	52%
We don't plan to address this	20%	30%	19%	15%	19%	30%	8%	24%	15%	16%	33%	12%	9%	19%	19%	40%	20%	12%	17%

CONTINUED ON NEXT PAGE

ACCESS RIGHTS AND CONTROLS–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
What are your plans related to documenting procedures for: –CONTINUED																			
System notifications to users (employees and customers) of appropriate usage obligations when logging into the firm's system.																			
I/We are actively working on this now	23%	23%	12%	27%	32%	18%	43%	21%	30%	5%	12%	36%	32%	17%	14%	17%	27%	24%	16%
I/We are not actively working on this, but plan to address it	44%	39%	48%	36%	52%	43%	35%	38%	40%	67%	45%	32%	43%	52%	43%	35%	37%	54%	48%
We don't plan to address this	33%	39%	40%	36%	16%	39%	22%	41%	30%	29%	42%	32%	25%	30%	43%	48%	35%	22%	36%
Devices used to access the firm's system externally.																			
I/We are actively working on this now	33%	32%	38%	38%	29%	21%	71%	40%	18%	22%	24%	33%	44%	57%	33%	24%	36%	40%	25%
I/We are not actively working on this, but plan to address it	41%	36%	31%	54%	47%	41%	21%	30%	64%	56%	32%	50%	31%	36%	50%	33%	36%	48%	50%
We don't plan to address this	26%	32%	31%	8%	24%	38%	7%	30%	18%	22%	44%	17%	25%	7%	17%	43%	27%	12%	25%
Encryption of devices used to access systems, including ability to remotely monitor, track, and deactivate devices.																			
I/We are actively working on this now	33%	35%	28%	50%	29%	24%	47%	40%	25%	42%	22%	41%	32%	41%	45%	22%	37%	32%	33%
I/We are not actively working on this, but plan to address it	45%	35%	44%	39%	59%	39%	35%	48%	58%	42%	44%	32%	50%	53%	45%	33%	42%	50%	56%
We don't plan to address this	22%	29%	28%	11%	12%	37%	18%	12%	17%	17%	33%	27%	18%	6%	9%	44%	21%	18%	11%
Customer complaints received by the firm related to customer access.																			
I/We are actively working on this now	25%	31%	26%	13%	30%	32%	50%	24%	7%	6%	31%	37%	33%	18%	0%	20%	32%	28%	15%
I/We are not actively working on this, but plan to address it	40%	31%	41%	44%	45%	32%	28%	38%	47%	63%	35%	37%	46%	29%	70%	30%	34%	48%	50%
We don't plan to address this	35%	38%	32%	44%	25%	35%	22%	38%	47%	31%	35%	26%	21%	53%	30%	50%	34%	24%	35%
Verification of the authenticity of customer requests to transfer funds.																			
I/We are actively working on this now	56%	50%	48%	67%	80%	56%	67%	82%	50%	29%	54%	58%	50%	78%	20%	44%	65%	50%	57%
I/We are not actively working on this, but plan to address it	22%	13%	39%	0%	0%	17%	22%	9%	17%	57%	23%	8%	40%	22%	40%	0%	30%	28%	14%
We don't plan to address this	22%	38%	13%	33%	20%	28%	11%	9%	33%	14%	23%	33%	10%	0%	40%	56%	5%	22%	29%
Reviews of employee access rights/restrictions regarding job-specific resources within the network.																			
I/We are actively working on this now	33%	26%	32%	39%	47%	29%	58%	30%	24%	25%	25%	42%	50%	31%	27%	29%	32%	39%	33%
I/We are not actively working on this, but plan to address it	40%	35%	47%	39%	18%	39%	21%	40%	47%	58%	36%	42%	35%	38%	55%	19%	50%	42%	38%
We don't plan to address this	27%	39%	21%	22%	35%	32%	21%	30%	29%	17%	39%	16%	15%	31%	18%	52%	18%	19%	29%
Internal audits conducted by the firm regarding access rights and controls.																			
I/We are actively working on this now	27%	26%	19%	35%	43%	22%	42%	31%	25%	21%	27%	21%	40%	31%	8%	29%	24%	35%	19%
I/We are not actively working on this, but plan to address it	47%	48%	51%	35%	43%	47%	37%	45%	69%	43%	42%	50%	52%	50%	50%	33%	49%	51%	52%
We don't plan to address this	25%	26%	30%	30%	14%	31%	21%	24%	6%	36%	30%	29%	8%	19%	42%	38%	27%	14%	29%

DATA LOSS PREVENTION

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
Do you have policies and procedures formally documented today as it relates to data loss prevention?																			
Yes	58%	54%	56%	66%	61%	48%	69%	60%	60%	65%	47%	61%	63%	63%	73%	46%	59%	63%	59%
No	24%	35%	22%	22%	8%	39%	17%	14%	16%	15%	40%	27%	20%	15%	15%	40%	27%	16%	15%
I don't know	19%	11%	22%	13%	31%	13%	14%	26%	24%	20%	14%	12%	17%	21%	12%	14%	14%	21%	26%
What are your plans related to documenting policies and procedures for data loss prevention?																			
I/We are actively working on this now	18%	16%	11%	42%	8%	10%	17%	29%	29%	37%	10%	11%	27%	20%	60%	13%	17%	17%	29%
I/We are not actively working on this, but plan to address it	64%	62%	72%	53%	67%	69%	57%	67%	50%	58%	68%	74%	62%	80%	40%	61%	68%	67%	61%
We don't plan to address this	18%	22%	18%	5%	25%	21%	26%	5%	21%	5%	23%	14%	12%	0%	0%	26%	14%	17%	11%
When was the bulk of that work completed?																			
Within last 6 months	29%	39%	28%	18%	26%	37%	32%	28%	17%	23%	32%	45%	24%	27%	22%	27%	38%	26%	22%
6 months–1 year	31%	31%	31%	29%	36%	21%	36%	40%	22%	33%	20%	17%	48%	33%	35%	33%	21%	35%	40%
1–2 years	24%	16%	27%	29%	24%	22%	16%	21%	39%	31%	23%	24%	17%	33%	35%	23%	19%	26%	26%
3 years+	13%	15%	11%	18%	10%	17%	16%	9%	17%	8%	18%	14%	11%	7%	9%	10%	21%	10%	10%
I don't know	3%	0%	3%	5%	5%	3%	0%	2%	4%	5%	7%	0%	0%	0%	0%	7%	1%	3%	2%
Which of the following do you have formally documented today as it relates to data loss prevention?																			
Policies and procedures related to monitoring unauthorized distribution of sensitive information outside of the firm (e.g. through email, physical media, hard copy)	67%	61%	75%	76%	64%	64%	57%	64%	69%	86%	63%	70%	64%	68%	74%	59%	61%	69%	77%
Policies and procedures related to enterprise data loss prevention and information	65%	66%	65%	68%	62%	61%	59%	72%	73%	64%	63%	66%	62%	84%	63%	74%	63%	68%	60%
I don't know	8%	4%	7%	7%	11%	7%	10%	4%	12%	7%	6%	6%	6%	0%	15%	0%	11%	9%	6%
None of the above	4%	7%	6%	0%	2%	8%	2%	4%	0%	2%	8%	4%	4%	3%	0%	12%	4%	3%	2%
Which of the following are included in your policies regarding enterprise data loss prevention?																			
Systems, utilities, and tools used to prevent, detect, and monitor data loss as it relates to PII and access to customer	63%	57%	64%	75%	63%	58%	62%	59%	74%	68%	50%	65%	77%	58%	76%	56%	60%	69%	64%
Data mapping: understanding information ownership	41%	37%	43%	54%	37%	29%	24%	35%	53%	64%	28%	29%	42%	38%	59%	32%	32%	42%	58%
Data mapping: how the firm documents or evidences personally identifiable information ("PII")	37%	26%	40%	50%	40%	31%	28%	26%	42%	57%	31%	29%	35%	23%	59%	28%	30%	42%	45%
I don't know	21%	24%	21%	11%	23%	24%	21%	29%	11%	14%	28%	19%	16%	23%	6%	12%	28%	23%	12%
None of the above	6%	13%	2%	4%	7%	7%	14%	9%	0%	0%	13%	6%	3%	8%	6%	20%	8%	0%	3%

CONTINUED ON NEXT PAGE

DATA LOSS PREVENTION–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4 –7	8+
Which of the following do you have in place related to enterprise data loss prevention?																			
Firm policies related to data classification	50%	40%	53%	57%	48%	44%	39%	50%	53%	59%	31%	65%	57%	27%	71%	36%	46%	55%	59%
Risk level associated with each category of data	35%	38%	30%	36%	38%	29%	21%	21%	42%	63%	25%	26%	43%	19%	65%	28%	26%	41%	44%
Factors considered when classifying data	30%	22%	32%	43%	34%	22%	29%	24%	32%	44%	16%	26%	50%	15%	35%	16%	24%	39%	38%
I don't know	25%	24%	30%	21%	24%	27%	18%	38%	16%	22%	34%	16%	17%	42%	6%	24%	26%	27%	19%
None of the above	13%	22%	9%	4%	14%	18%	25%	12%	5%	4%	25%	13%	13%	12%	6%	28%	20%	4%	6%
What are your plans related to documenting policies and procedures for:																			
Policies and procedures related to enterprise data loss prevention and information.																			
I/We are actively working on this now	15%	10%	21%	10%	23%	13%	20%	0%	0%	33%	13%	8%	19%	0%	0%	22%	5%	18%	22%
I/We are not actively working on this, but plan to address it	65%	81%	58%	60%	46%	67%	73%	70%	75%	42%	69%	77%	63%	80%	67%	67%	86%	59%	44%
We don't plan to address this	20%	10%	21%	30%	31%	21%	7%	30%	25%	25%	19%	15%	19%	20%	33%	11%	10%	24%	33%
Policies and procedures related to monitoring unauthorized distribution of sensitive information outside of the firm.																			
I/We are actively working on this now	27%	13%	42%	43%	25%	18%	29%	33%	40%	33%	13%	36%	38%	20%	33%	14%	29%	31%	33%
I/We are not actively working on this, but plan to address it	58%	70%	42%	57%	50%	64%	50%	53%	60%	67%	63%	55%	38%	70%	67%	71%	48%	69%	44%
We don't plan to address this	15%	17%	17%	0%	25%	18%	21%	13%	0%	0%	25%	9%	23%	10%	0%	14%	24%	0%	22%

VENDOR MANAGEMENT

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
Do you have policies and procedures formally documented today as it relates to vendor management?																			
Yes	43%	38%	43%	56%	43%	30%	48%	50%	47%	56%	29%	46%	47%	55%	60%	25%	42%	49%	51%
No	35%	53%	28%	26%	18%	53%	33%	22%	27%	16%	54%	39%	32%	23%	24%	58%	39%	26%	20%
I don't know	23%	9%	29%	18%	39%	16%	20%	28%	26%	28%	17%	15%	21%	23%	16%	17%	19%	25%	29%
What are your plans related to documenting policies and procedures for vendor management? (if not in place now)																			
I/We are actively working on this now	12%	8%	7%	41%	8%	6%	14%	18%	22%	30%	6%	8%	24%	23%	25%	2%	13%	19%	19%
I/We are not actively working on this, but plan to address it	49%	47%	60%	27%	50%	46%	47%	52%	61%	55%	43%	51%	45%	64%	56%	40%	52%	53%	56%
We don't plan to address this	40%	44%	33%	32%	42%	48%	40%	30%	17%	15%	51%	41%	31%	14%	19%	57%	35%	29%	25%
When was the bulk of that work completed?																			
Within last 6 months	32%	41%	28%	28%	31%	41%	39%	33%	18%	22%	46%	39%	30%	29%	20%	54%	43%	22%	23%
6 months–1 year	31%	21%	35%	33%	31%	23%	35%	30%	29%	36%	13%	29%	37%	43%	30%	8%	17%	40%	43%
1–2 years	23%	26%	19%	28%	22%	18%	17%	27%	29%	31%	17%	23%	26%	14%	40%	23%	22%	22%	28%
3 years+	13%	12%	19%	8%	13%	18%	9%	10%	24%	6%	25%	10%	7%	14%	5%	15%	17%	14%	5%
I don't know	1%	0%	0%	3%	3%	0%	0%	0%	0%	6%	0%	0%	0%	0%	5%	0%	0%	2%	3%
Which of the following do you have formally documented information, policies or procedures?																			
Vendors with access to the firm's network or data	70%	58%	64%	84%	74%	57%	58%	73%	80%	83%	56%	61%	70%	73%	81%	40%	65%	70%	86%
Third-party vendors	68%	66%	60%	84%	63%	64%	65%	67%	50%	86%	52%	67%	70%	68%	81%	60%	65%	72%	70%
Third-party vendors that facilitate the mitigation of cybersecurity risks	46%	34%	47%	51%	49%	33%	46%	48%	40%	58%	33%	42%	50%	45%	48%	27%	47%	48%	49%
Sample documents or notices required of third-party vendors	39%	34%	30%	41%	49%	29%	38%	30%	30%	58%	26%	36%	37%	27%	67%	27%	31%	46%	42%
Contingency plans for vendors	35%	34%	38%	32%	31%	38%	31%	30%	30%	39%	44%	27%	33%	27%	38%	47%	35%	33%	33%
I don't know	4%	3%	6%	3%	6%	2%	4%	9%	10%	0%	7%	0%	7%	5%	5%	7%	4%	4%	5%
None of the above	3%	8%	2%	0%	3%	5%	8%	0%	5%	0%	4%	6%	3%	0%	0%	7%	2%	4%	2%
Which of the following are included in your policies related to third-party vendors?																			
Contracts, agreements, and the related approval process	82%	92%	68%	87%	76%	85%	71%	76%	90%	84%	86%	82%	76%	71%	76%	89%	91%	67%	90%
Due diligence with regard to vendor selection	80%	84%	79%	81%	76%	81%	65%	90%	100%	74%	86%	82%	76%	79%	71%	67%	84%	79%	79%
Risk assessments, risk management, and performance measurements required of vendors	61%	76%	57%	65%	43%	63%	53%	52%	80%	65%	57%	59%	57%	64%	82%	56%	53%	64%	69%
Supervision, monitoring, tracking and access control	56%	60%	57%	58%	43%	52%	41%	57%	40%	68%	43%	55%	67%	36%	71%	22%	59%	56%	62%
I don't know	6%	4%	7%	0%	14%	0%	12%	5%	0%	10%	0%	5%	5%	7%	12%	0%	0%	13%	3%
None of the above	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

CONTINUED ON NEXT PAGE

VENDOR MANAGEMENT–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
What are your plans related to documenting policies and procedures for:																			
Third-party vendors.																			
I/We are actively working on this now	33%	18%	31%	40%	45%	23%	25%	38%	50%	20%	30%	18%	29%	33%	0%	50%	20%	23%	55%
I/We are not actively working on this, but plan to address it	47%	45%	50%	60%	36%	38%	50%	38%	50%	80%	50%	36%	71%	33%	100%	25%	33%	69%	45%
We don't plan to address this	21%	36%	19%	0%	18%	38%	25%	25%	0%	0%	20%	45%	0%	33%	0%	25%	47%	8%	0%
Vendors with access to the firm's network or data.																			
I/We are actively working on this now	29%	29%	29%	17%	43%	25%	50%	17%	0%	33%	11%	31%	43%	33%	33%	29%	20%	43%	20%
I/We are not actively working on this, but plan to address it	32%	21%	36%	50%	29%	38%	10%	50%	33%	33%	56%	23%	43%	17%	33%	43%	20%	43%	20%
We don't plan to address this	39%	50%	36%	33%	29%	38%	40%	33%	67%	33%	33%	46%	14%	50%	33%	29%	60%	14%	60%
Third-party vendors that facilitate the mitigation of cybersecurity risks.																			
I/We are actively working on this now	34%	39%	27%	41%	31%	31%	31%	43%	10%	47%	27%	42%	38%	18%	30%	22%	38%	38%	30%
I/We are not actively working on this, but plan to address it	38%	17%	36%	53%	50%	19%	46%	36%	70%	47%	13%	32%	38%	55%	60%	11%	33%	38%	55%
We don't plan to address this	28%	43%	36%	6%	19%	50%	23%	21%	20%	7%	60%	26%	23%	27%	10%	67%	29%	23%	15%
Contingency plans for vendors.																			
I/We are actively working on this now	25%	22%	19%	38%	23%	21%	29%	30%	8%	32%	8%	33%	28%	20%	33%	50%	30%	18%	22%
I/We are not actively working on this, but plan to address it	45%	39%	42%	54%	41%	29%	41%	50%	67%	50%	33%	38%	50%	53%	67%	0%	27%	62%	56%
We don't plan to address this	30%	39%	38%	8%	36%	50%	29%	20%	25%	18%	58%	29%	22%	27%	0%	50%	43%	21%	22%
Sample documents or notices required of third-party vendors.																			
I/We are actively working on this now	26%	30%	17%	38%	20%	29%	27%	26%	17%	27%	18%	33%	29%	29%	17%	44%	28%	19%	23%
I/We are not actively working on this, but plan to address it	44%	35%	50%	43%	47%	25%	47%	63%	58%	47%	35%	38%	53%	50%	50%	11%	41%	63%	41%
We don't plan to address this	30%	35%	33%	19%	33%	46%	27%	11%	25%	27%	47%	29%	18%	21%	33%	44%	31%	19%	36%

INCIDENT RESPONSE

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
Do you have policies and procedures formally documented today as it relates to incident response?																			
Yes	43%	34%	45%	58%	48%	30%	46%	50%	51%	57%	32%	39%	44%	51%	58%	28%	41%	49%	50%
No	34%	54%	28%	25%	16%	53%	33%	21%	32%	17%	52%	38%	34%	21%	28%	57%	38%	24%	22%
I don't know	23%	12%	27%	18%	36%	18%	21%	29%	18%	26%	15%	23%	21%	28%	13%	15%	20%	26%	27%
What are your plans related to documenting policies and procedures for incident response? (if not in place now)																			
I/We are actively working on this now	14%	10%	11%	24%	27%	10%	16%	19%	22%	29%	8%	12%	18%	25%	26%	8%	15%	16%	25%
I/We are not actively working on this, but plan to address it	61%	60%	63%	71%	55%	58%	53%	74%	63%	62%	57%	63%	64%	70%	63%	57%	57%	71%	63%
We don't plan to address this	25%	29%	26%	5%	18%	32%	30%	6%	15%	10%	36%	24%	18%	5%	11%	35%	28%	13%	13%
When was the bulk of that work completed?																			
Within last 6 months	27%	39%	23%	30%	18%	27%	39%	28%	17%	24%	38%	25%	31%	28%	28%	43%	28%	23%	25%
6 months–1 year	37%	36%	41%	33%	32%	30%	39%	40%	39%	41%	14%	29%	52%	39%	28%	21%	40%	36%	42%
1–2 years	25%	21%	23%	27%	32%	30%	14%	20%	39%	24%	29%	38%	10%	33%	33%	21%	19%	30%	28%
3 years+	7%	3%	10%	6%	7%	10%	7%	8%	0%	9%	10%	8%	7%	0%	11%	7%	12%	6%	3%
I don't know	4%	0%	3%	3%	11%	3%	0%	4%	6%	3%	10%	0%	0%	0%	0%	7%	2%	4%	3%
Which of the following do you have formally documented today as it relates to incident response?																			
Business continuity plan in case of cybersecurity incident	75%	83%	65%	86%	70%	68%	80%	69%	77%	84%	66%	74%	72%	77%	84%	78%	69%	76%	81%
Incidents of unauthorized internal or external distributions of PII	36%	33%	25%	57%	38%	28%	30%	28%	36%	57%	28%	26%	31%	50%	42%	28%	31%	36%	45%
Actual customer losses associated with cyber incidents	36%	33%	29%	43%	43%	33%	17%	31%	36%	54%	24%	26%	25%	50%	42%	17%	33%	42%	38%
Process to test incident response plan	29%	25%	24%	37%	30%	13%	30%	28%	36%	43%	10%	30%	34%	14%	58%	17%	29%	31%	31%
System-generated alerts related to data loss of sensitive/ confidential information	28%	28%	25%	26%	32%	20%	13%	22%	32%	46%	21%	22%	22%	23%	47%	11%	31%	22%	38%
Successful unauthorized internal or external incidents related to access	28%	28%	24%	40%	27%	15%	20%	28%	32%	46%	14%	26%	25%	41%	37%	11%	29%	29%	33%
I don't know	11%	3%	20%	3%	19%	13%	7%	22%	14%	5%	17%	7%	9%	18%	0%	22%	8%	13%	10%
None of the above	4%	6%	4%	3%	5%	13%	0%	0%	5%	3%	10%	4%	0%	0%	5%	0%	8%	2%	5%

CONTINUED ON NEXT PAGE

INCIDENT RESPONSE–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
Which of the following are included in your policies related to business continuity and incident reporting?																			
Processes to mitigate the effects of a cybersecurity incident	85%	90%	82%	93%	73%	81%	88%	91%	76%	87%	84%	85%	91%	76%	88%	86%	89%	86%	79%
Responsibility for losses associated with attacks or intrusions impacting clients	59%	57%	48%	77%	58%	59%	46%	55%	59%	71%	47%	65%	61%	53%	63%	57%	54%	60%	65%
I don't know	6%	0%	12%	0%	15%	4%	4%	5%	18%	3%	0%	10%	0%	12%	13%	7%	3%	10%	6%
None of the above	5%	3%	6%	0%	8%	7%	8%	5%	6%	0%	11%	0%	9%	6%	0%	7%	3%	5%	6%
Which of the following are included in your policies related to business continuity and incident reporting?																			
Processes to mitigate the effects of a cybersecurity incident	85%	90%	82%	93%	73%	81%	88%	91%	76%	87%	84%	85%	91%	76%	88%	86%	89%	86%	79%
Responsibility for losses associated with attacks or intrusions impacting clients	59%	57%	48%	77%	58%	59%	46%	55%	59%	71%	47%	65%	61%	53%	63%	57%	54%	60%	65%
I don't know	6%	0%	12%	0%	15%	4%	4%	5%	18%	3%	0%	10%	0%	12%	13%	7%	3%	10%	6%
None of the above	5%	3%	6%	0%	8%	7%	8%	5%	6%	0%	11%	0%	9%	6%	0%	7%	3%	5%	6%
Which of the following do you have in place related to customer losses associated with cyber incdents?																			
Whether the firm had cybersecurity insurance coverage, including the types of incidents the insurance covered	63%	75%	60%	67%	50%	77%	20%	70%	50%	65%	86%	57%	63%	45%	63%	100%	76%	48%	63%
Whether any insurance claims related to cyber events were filed	47%	58%	47%	47%	44%	69%	20%	60%	25%	40%	71%	57%	63%	27%	38%	100%	65%	39%	31%
Amount of cyber-related losses recovered pursuant to the firm's cybersecurity insurance coverage	47%	50%	67%	47%	31%	69%	0%	80%	13%	45%	86%	29%	75%	36%	25%	67%	71%	35%	38%
Amount of customer losses reimbursed by the firm	39%	42%	53%	40%	25%	38%	0%	50%	25%	55%	71%	0%	63%	27%	38%	67%	35%	30%	50%
I don't know	19%	8%	27%	13%	25%	8%	40%	10%	38%	15%	0%	29%	13%	18%	25%	0%	6%	35%	13%
None of the above	10%	17%	0%	13%	13%	15%	20%	0%	13%	10%	14%	14%	0%	18%	13%	0%	12%	9%	13%
What are your plans related to documenting policies and procedures for:																			
Business continuity plan in case of cybersecurity incident.																			
I/We are actively working on this now	40%	33%	33%	67%	0%	33%	50%	0%	100%	67%	50%	25%	33%	0%	100%	0%	38%	20%	100%
I/We are not actively working on this, but plan to address it	60%	67%	67%	33%	100%	67%	50%	100%	0%	33%	50%	75%	67%	100%	0%	0%	63%	80%	0%
We don't plan to address this	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Process to test incident response plan.																			
I/We are actively working on this now	22%	21%	15%	40%	18%	20%	26%	13%	10%	33%	17%	38%	17%	13%	71%	9%	29%	17%	26%
I/We are not actively working on this, but plan to address it	52%	63%	52%	45%	47%	52%	47%	63%	70%	44%	61%	44%	67%	60%	14%	45%	50%	57%	52%
We don't plan to address this	26%	17%	33%	15%	35%	28%	26%	25%	20%	22%	22%	19%	17%	27%	14%	45%	21%	27%	22%

CONTINUED ON NEXT PAGE

INCIDENT RESPONSE–CONTINUED

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGE-MENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4 –7	8+
What are your plans related to documenting policies and procedures for: –CONTINUED																			
System-generated alerts related to data loss of sensitive/confidential information.																			
I/We are actively working on this now	19%	22%	19%	21%	13%	27%	29%	6%	0%	24%	13%	33%	23%	8%	33%	17%	22%	20%	15%
I/We are not actively working on this, but plan to address it	47%	43%	46%	46%	56%	32%	50%	50%	73%	41%	40%	44%	55%	54%	22%	25%	44%	57%	45%
We don't plan to address this	34%	35%	35%	33%	31%	41%	21%	44%	27%	35%	47%	22%	23%	38%	44%	58%	33%	23%	40%
Incidents of unauthorized internal or external distributions of PII																			
I/We are actively working on this now	30%	29%	38%	31%	21%	16%	42%	13%	30%	54%	15%	29%	32%	14%	50%	33%	19%	37%	35%
I/We are not actively working on this, but plan to address it	49%	52%	38%	54%	43%	53%	42%	56%	70%	31%	46%	65%	53%	43%	40%	22%	63%	48%	41%
We don't plan to address this	21%	19%	23%	15%	36%	32%	16%	31%	0%	15%	38%	6%	16%	43%	10%	44%	19%	15%	24%
Successful unauthorized internal or external incidents related to access																			
I/We are actively working on this now	29%	35%	33%	21%	28%	21%	36%	25%	18%	35%	18%	18%	43%	22%	36%	17%	32%	35%	23%
I/We are not actively working on this, but plan to address it	54%	61%	41%	63%	50%	54%	50%	63%	73%	47%	53%	71%	48%	67%	36%	42%	61%	55%	50%
We don't plan to address this	17%	4%	26%	16%	22%	25%	14%	13%	9%	18%	29%	12%	10%	11%	27%	42%	7%	10%	27%
Actual customer losses associated with cyber incidents																			
I/We are actively working on this now	25%	29%	25%	22%	25%	12%	39%	13%	20%	36%	0%	47%	19%	14%	30%	18%	19%	29%	30%
I/We are not actively working on this, but plan to address it	53%	48%	46%	67%	50%	53%	48%	60%	70%	50%	57%	35%	52%	86%	50%	45%	62%	54%	45%
We don't plan to address this	22%	24%	29%	11%	25%	35%	13%	27%	10%	14%	43%	18%	29%	0%	20%	36%	19%	17%	25%

TRAINING

	ALL RESPONDENTS	ROLE				ASSETS UNDER MANAGEMENT					GROSS REVENUE (IN LAST 12 MONTHS)					NUMBER OF TEAM MEMBERS			
		CEO	ADVISER	NON-ADVISER MANAGEMENT	SUPPORT STAFF	LESS THAN $50M	$50M–$99.9M	$100M–$249.9M	$250M–$499.9M	$500M+	LESS THAN $250K	$250K–$499.9K	$500K–$999.9K	$1M–$2.49M	$2.5M+	1	2–3	4–7	8+
Do you provide employee or vendor training regarding information and security risks?																			
Yes	51%	54%	49%	63%	46%	39%	49%	53%	58%	60%	39%	54%	46%	56%	66%	0%	42%	52%	60%
No	33%	40%	31%	30%	29%	50%	41%	27%	30%	20%	48%	41%	42%	26%	26%	0%	47%	27%	24%
I don't know	16%	6%	20%	7%	25%	11%	10%	20%	12%	20%	14%	5%	12%	18%	8%	0%	10%	21%	16%
What are your plans related to documenting policies and procedures for employee training? (if not in place now)																			
I/We are actively working on this now	20%	14%	16%	32%	24%	11%	30%	23%	16%	25%	2%	16%	26%	32%	12%	0%	21%	13%	26%
I/We are not actively working on this, but plan to address it	50%	56%	51%	52%	39%	53%	40%	54%	60%	46%	60%	49%	45%	52%	59%	0%	44%	58%	56%
We don't plan to address this	30%	30%	33%	16%	37%	36%	30%	23%	24%	29%	38%	36%	28%	16%	29%	0%	35%	29%	19%
When was the bulk of that work completed?																			
Within last 6 months	26%	32%	22%	25%	28%	31%	33%	21%	13%	26%	27%	38%	31%	6%	35%	0%	34%	23%	21%
6 months–1 year	47%	42%	46%	56%	40%	35%	43%	46%	56%	57%	13%	42%	41%	75%	47%	0%	32%	50%	60%
1–2 years	15%	16%	14%	14%	20%	15%	14%	14%	19%	14%	20%	19%	14%	13%	12%	0%	16%	20%	9%
3 years+	10%	10%	19%	3%	8%	19%	10%	14%	6%	3%	40%	0%	14%	6%	6%	0%	18%	7%	5%
I don't know	2%	0%	0%	3%	4%	0%	0%	4%	6%	0%	0%	0%	0%	0%	0%	0%	0%	0%	5%
Which of the following do you have formally documented today?																			
Training provided to your team regarding information security and risks	79%	83%	80%	85%	69%	76%	81%	77%	65%	95%	78%	81%	85%	73%	89%	0%	83%	74%	82%
Training provided to third-party vendors or business partners related to information security	13%	14%	13%	13%	11%	12%	8%	9%	13%	14%	17%	10%	12%	0%	26%	0%	10%	18%	10%
I don't know	12%	8%	11%	8%	23%	6%	19%	14%	17%	5%	0%	10%	15%	18%	5%	0%	8%	18%	10%
None of the above	6%	6%	9%	3%	6%	15%	0%	6%	13%	0%	17%	6%	0%	9%	5%	0%	8%	5%	6%
What are your plans related to documenting policies and procedures for :																			
Training provided to your team regarding information security and risks.																			
I/We are actively working on this now	21%	33%	50%	0%	0%	17%	0%	67%	0%	0%	25%	0%	0%	50%	0%	0%	20%	40%	0%
I/We are not actively working on this, but plan to address it	64%	33%	25%	100%	100%	50%	0%	33%	100%	0%	50%	67%	0%	50%	100%	0%	40%	60%	100%
We don't plan to address this	14%	33%	25%	0%	0%	33%	0%	0%	0%	0%	25%	33%	0%	0%	0%	0%	40%	0%	0%
Training provided to third-party vendors or business partners related to information security.																			
I/We are actively working on this now	10%	0%	20%	9%	9%	7%	5%	19%	0%	13%	7%	8%	16%	6%	0%	0%	7%	11%	12%
I/We are not actively working on this, but plan to address it	36%	43%	26%	34%	39%	33%	21%	41%	44%	37%	47%	24%	32%	44%	15%	0%	30%	46%	32%
We don't plan to address this	55%	57%	54%	56%	52%	59%	74%	41%	56%	50%	47%	68%	52%	50%	85%	0%	63%	43%	56%

FPA FINANCIAL PLANNING ASSOCIATION

Research & Practice Institute™

Sponsored by TD Ameritrade Institutional

Contact

If you are a member of the media and are interested in interviewing an FPA leader about this report, or need assistance securing additional research, please contact:

FPA

BEN LEWIS

FPA Director of Public Relations

303-867-7190

BLewis@OneFPA.org