FPA FINANCIAL PLANNING ASSOCIATION

RESEARCH & PRACTICE INSTITUTE™

Sponsored By

TD Ameritrade Institutional

CYBERSECURITY WHITEPAPER

Client Perception and Communication

CYBERSECURITY: CLIENT PERCEPTION AND COMMUNICATION

Introduction

New research released in September 2016 underscored the critical importance of cybersecurity issues for advisory firms. According to the study, from the FPA Research and Practice Institute™ and sponsored by TD Ameritrade Institutional, 81 percent of respondents say that cybersecurity is high or very high among their firm's priorities.

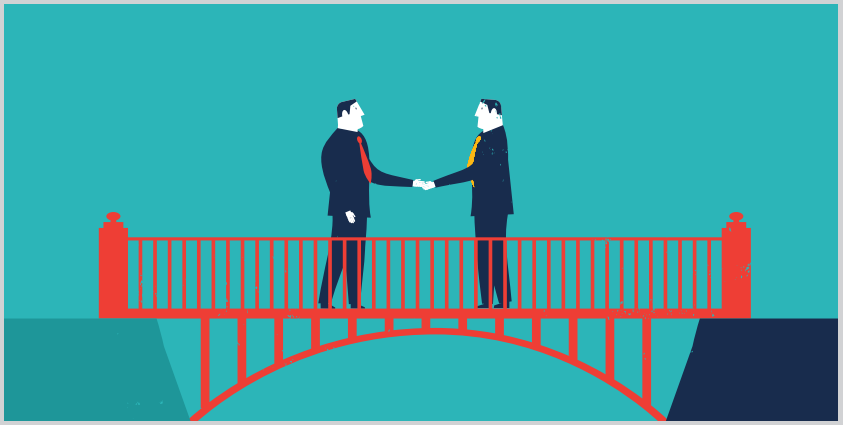
The initial report focused on the numbers, examining where advisers are today in meeting cybersecurity requirements as set forth by OCIE (the Securities and Exchange Commission's Office of Compliance Inspections and Examinations) and where there are gaps. This is the first in a series of three whitepapers that will focus on the tactical issues associated with cybersecurity, including client communication, team training and best technology practices. In this whitepaper we'll shift the focus from the internal requirements to the ways in which advisers are communicating with clients on this issue.

	CRITICAL QUESTION	WHITEPAPER PUB DATE
✓	Client Perception and Communication	October 2016
✓	Is Your Team Prepared?	November 2016
✓	Cybersecurity: Current Threats and Risk Management	December 2016

CYBERSECURITY: CLIENT PERCEPTION AND COMMUNICATION

Perception and Role

When sharing any research data, the averages tell an important story; however, some of the most interesting insights are generated by segmenting the data. When it comes to perception of client awareness or concern, views change depending on the role the respondent plays in the firm. That is, there are striking differences in views between the CEO of a firm and both non-adviser management and support staff.



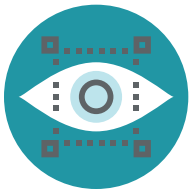
The differences may result from the team being on the receiving end of client questions or being tasked with making the necessary changes to comply with OCIE requirements. Either way, the data suggests that there are differences of opinion across teams which may need to be bridged.

CYBERSECURITY: CLIENT PERCEPTION AND COMMUNICATION

Awareness

The data is clear that cybersecurity is a priority for those in the financial advisory space. Despite the perceived level of importance, we also know that many firms do not feel fully prepared. Forty-four percent of respondents 'completely agree' that they fully understand the issues and risks associated with cybersecurity. That drops to 36 percent when they reflect on their team's understanding.

In this paper, however, we are shifting from adviser and team awareness to client awareness. Simply stated, respondents do not believe clients are well versed on the issues associated with cybersecurity. According to respondents, only 11 percent of clients are 'very aware' of the general risks associated with data security, although a further 59 percent, they believe, are somewhat aware. Non-adviser management and support staff believe that clients have higher levels of awareness, but agree they are not fully aware of the risks.



CYBERSECURITY: CLIENT PERCEPTION AND COMMUNICATION

Awareness

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

	ALL RESPONDANTS	NOT WORKING ON THIS BUT PLAN TO ADDRESS IT	NON-ADVISER MANAGEMENT	SUPPORT STAFF
Somewhat aware	59%	52%	65%	61%
Very aware	11%	10%	10%	14%

When asked about the specific requirements being mandated for advisers by OCIE, respondents felt clients had even lower levels of awareness. While respondents believe 70 percent of clients are somewhat or very aware of the general risks, they believe that only 14 percent are aware of the requirements that are specific to this industry. Once again teams tend to believe clients are more aware of the specifics.

QUESTION: To the best of your knowledge, are your clients aware of the requirements being mandated for you to deal with cybersecurity risks?

	ALL RESPONDANTS	CEO	NON-ADVISER MANAGEMENT	SUPPORT STAFF
Yes	14%	9%	24%	19%
No	63%	74%	58%	49%
I don't know	23%	18%	19%	33%

It is interesting to note that 23 percent of respondents say they simply don't know if clients are aware of the requirements, climbing to 33 percent among support staff. The data suggests that our perceptions of awareness may be, at least somewhat, influenced by a lack of real data on this issue.

CYBERSECURITY: CLIENT PERCEPTION AND COMMUNICATION

Perceived Concern

It would make sense that if respondents do not believe clients are aware of the issues, that they would also believe that they are not highly concerned. This is the case with respondents estimating that 11 percent of clients are ‘very worried’ about security breaches.

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

	ALL RESPONDANTS	CEO	NON-ADVISER MANAGEMENT	SUPPORT STAFF
Somewhat worried	52%	49%	58%	45%
Very worried	11%	12%	6%	10%

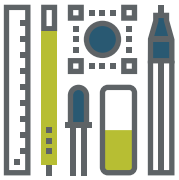
CYBERSECURITY: CLIENT PERCEPTION AND COMMUNICATION

Awareness

In February 2016, Kaspersky Lab, a global cybersecurity firm, surveyed 11,000 consumers on the subject of data security. That study found that nearly two-thirds (65%) of consumers worry about the data security practices of companies to which they provide personal and financial information, an increase of nine-percent over the previous year.

Whatever the source, the data suggests that clients are concerned about data security. Despite that concern, only a third of respondents said that clients had asked about how their adviser's firm was dealing with cybersecurity risks. According to the data, clients are less likely to ask the CEO about the issues than other team members.

QUESTION: To the best of your knowledge, are your clients aware of the requirements being mandated for you to deal with cybersecurity risks?



CYBERSECURITY: CLIENT PERCEPTION AND COMMUNICATION

Your Role in Educating Clients

Whether or not clients are asking questions directly, respondents do recognize the concern and believe that they have a role in educating clients on this topic. Respondents say that educating clients is somewhat important (42%) or very important (39%). Larger teams tend to place greater emphasis on the importance of educating clients. Non-adviser management and support teams also see client education as relatively more important than those in a CEO role.

QUESTION: How important is it that you educate your clients on the risk associated with data security?

	ALL RESPONDANTS	CEO	NON-ADVISER MANAGEMENT	SUPPORT STAFF
Somewhat Important	42%	43%	37%	38%
Very Important	39%	35%	48%	49%

CYBERSECURITY: CLIENT PERCEPTION AND COMMUNICATION

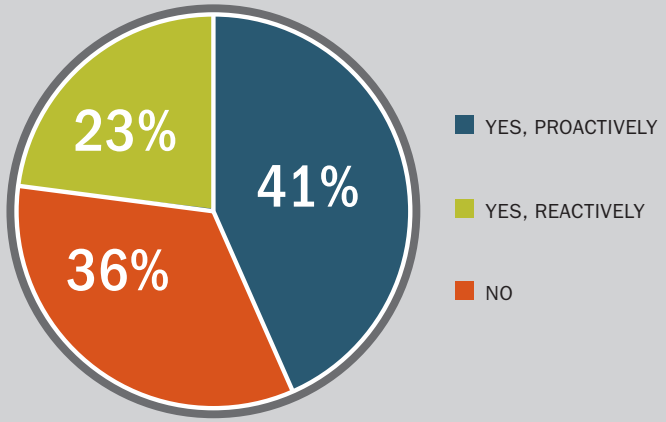
The Communication Process

While respondents are in agreement that education is important, the way in which that education is delivered varies greatly. Only 41 percent of respondents indicate that they have communicated proactively with clients about the risks.

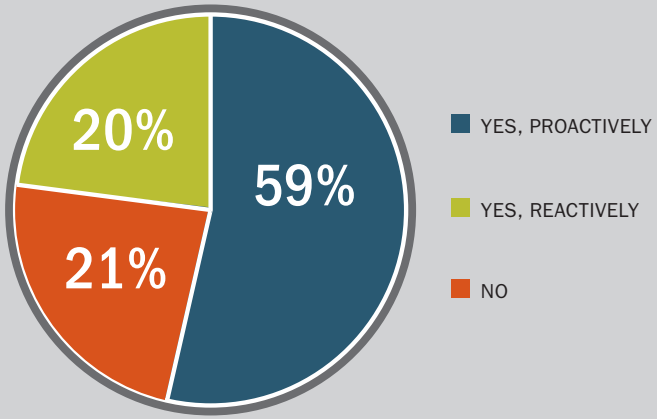
A clear gap emerges on this point. Among those respondents who feel that educating clients is very important, 41 percent did not communicate proactively.

QUESTION: Have you communicated with clients about how you are dealing with cybersecurity risks?

ALL RESPONDANTS



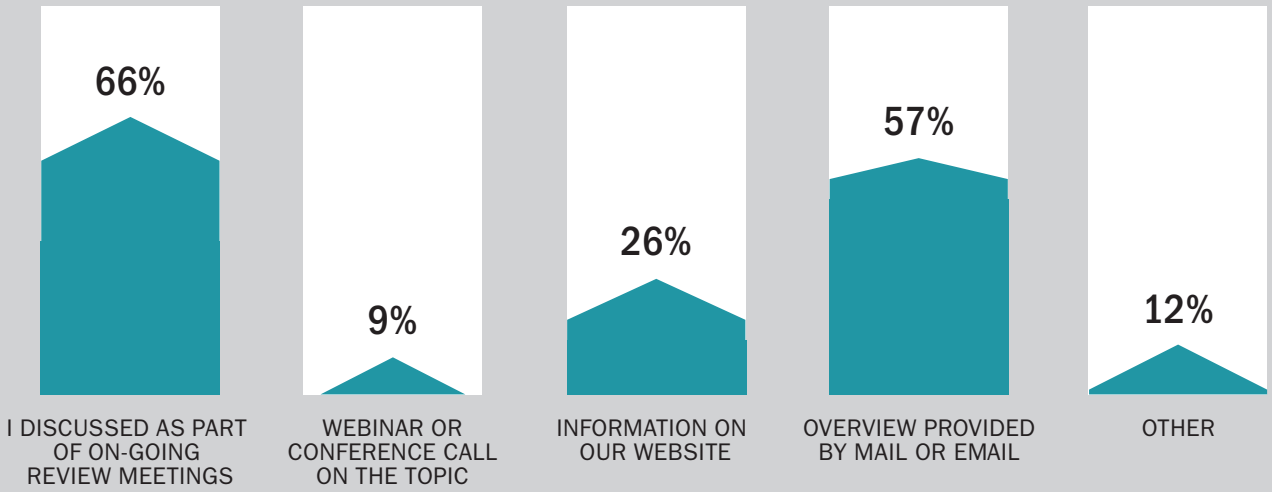
PERCENTAGE OF RESPONDANTS WHO BELIEVE THAT EDUCATING CLIENTS IS 'VERY IMPORTANT'



The Communication Process

A majority of respondents who are communicating on these issues are doing so one-on-one during client reviews; however, nearly 60 percent have sent out some form of written communication. Respondents are much less likely to put information on their site or hold webinars or conference calls on the issue.

QUESTION: How have you communicated with clients? Please select all that apply. (n=those who have communicated proactively or reactively with clients)

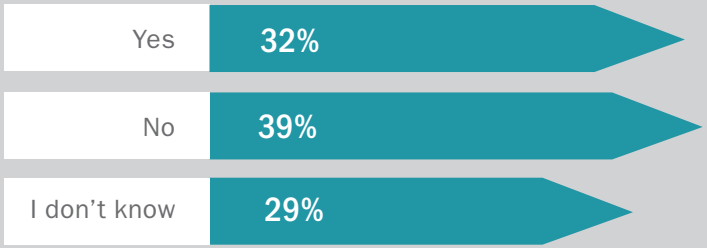


CYBERSECURITY: CLIENT PERCEPTION AND COMMUNICATION

Opportunity

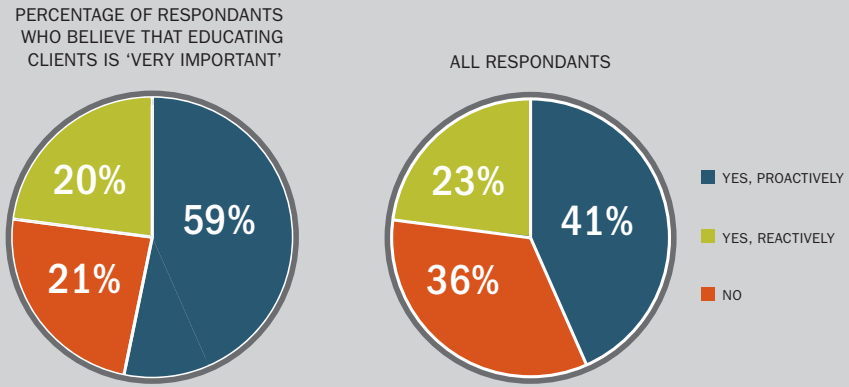
The data suggests that there is an opportunity to be more proactive in educating clients on the general risks associated with data security and the more specific requirements imposed on advisory firms. While most advisers are actively focused on ensuring they have the systems and procedures in place to meet the requirements set out by OCIE, some are actively involving their clients in the discussion as well. Nearly a third of respondents (32%) believe that their approach to dealing with cybersecurity is a competitive advantage.

Question: Do you feel your approach to dealing with cybersecurity risks is a competitive advantage relative to other advisors?



The extent to which this was seen as a competitive advantage is tied to being proactive. Among those who felt their approach was a competitive advantage, 61 percent had communicated proactively. When advisers did not see it as a competitive advantage they were more than twice as likely to say that had not communicated with clients on this issue.

Question: Have you communicated with clients about how you are dealing with cybersecurity risks?



Steps to Take Action

There are several things that we know to be true when it comes to cybersecurity. The risks are real, the requirements for your business are clear and clients are concerned. For that reason, we suggest the following action plan to help you gain clarity and move forward proactively.

1.TEAM MEETING.
The differences in response based on role suggest that teams could benefit by coming together and sharing what they are hearing from clients. What questions do they receive? Do they sense concern or worry? By tapping into the experience of everyone on the team and ensuring everyone is on the same page, you can move forward with a more focused plan.

2. GATHER DATA.
It seems clear that we do not have sufficient hard data on the level of awareness or concern among clients. By being proactive in gathering that information you will know if there are gaps and can get out ahead of the issue. Consider a simple survey on this one topic and use the results to inform your communications plan.

3. DECIDE ON YOUR ROLE.
On the basis of input from the team and your clients, determine the role you want to play in educating clients. Do you want to be proactive and position this as a way to add value or do you prefer to be more reactive in your approach while still ensuring that you are doing what is required internally?

4. MAP OUT YOUR COMMUNICATIONS PLAN.
Think about how you will communicate proactively with clients, if you have decided that is the best approach. Remember that one communication is never enough and you may need to find different way to get the same message across. Look across the full range of options including emails, blog posts, articles or other information on your site or a webinar or conference call.

5. FOCUS ON CONSISTENCY.
Whether or not you choose to be proactive, every advisory firm needs to be prepared to react appropriately. A decision to be reactive is not a decision to avoid the issue. As a firm, know that every team member is aware of the issues and responding in exactly the same way. Map out how you want the team to respond to questions, create a follow-up that can be sent to clients who do ask questions and bring the team together so that everyone is delivering the same message.

In the next whitepaper we'll focus on exactly how firms are training and communicating with their teams on this critical issue.

CYBERSECURITY: CLIENT PERCEPTION AND COMMUNICATION

Methodology and Participant Profile

This whitepaper and the original 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. 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 +/- 3.07%

The following provides a profile of the respondents included in this whitepaper and the original report.

QUESTION: Which of the following best describes your role?

CEO	31%
SENIOR/JUNIOR ADVISER	32%
NON-ADVISER MANAGEMENT	12%
SUPORT STAFF	20%
OTHER	5%

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

Yes, I have overall responsibility for policies and procedures	25%
Yes, I have overall responsibility for the execution policies and procedures	24%
Yes, I have overall responsibility and manage the execution of policies and procedures	31%
No	20%

QUESTION: What are your assets under management today?

Less than $50m	32%
$50-$99.9m	18%
$100-$249.9m	19%
$250-$499.9m	12%
$500M+	16%
$250-$499.9m	4%

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

Less than $250k	23%
$250k-$499.9k	16%
$500k-$999.9k	17%
$1m-$2.49m	12%
$2.5m+	16%
Not applicable/Prefer not to answer	20%

FPA FINANCIAL PLANNING ASSOCIATION

RESEARCH & PRACTICE INSTITUTE™

Sponsored By

TD Ameritrade Institutional

Be sure to download and review **Is Your Data Safe? The 2016 Financial Adviser Cybersecurity Assessment** to see how you compare to your peers in the financial advisory profession. Access the assessment today at

www.OneFPA.org/Cybersecurity