



CYBERSECURITY WHITEPAPER




Is Your Team Prepared?

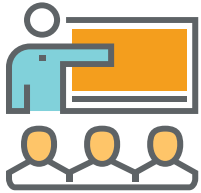
CYBERSECURITY: IS YOUR TEAM PREPARED?

Introduction

In September 2016 the FPA Research and Practice Institute™ released a study that was sponsored by TD Ameritrade Institutional and highlighted the critical importance that advisory firms place on managing cybersecurity risks. The initial report provided a quantitative overview of how advisers are taking action to manage those risks today and their plans going forward.

This is the second in a series of three whitepapers that focus on the tactical issues associated with cybersecurity, including client communication, team training and best technology practices. In this whitepaper we'll specifically focus on how firms are structuring and training their teams to be fully prepared to protect both firm and client data. You will find details on methodology and a participant profile at the end of this paper.

| | 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: IS YOUR TEAM PREPARED?

The Training Gap

The data makes it clear that the level of training provided to teams does not adequately reflect the level of importance placed on dealing with cybersecurity issues. Despite the fact that respondents say that overall team knowledge of the issues and requirements is relatively low, fewer than half of firms with more than one team member provide mandatory training.

The need for effective team training on cybersecurity issues is underscored by the following:

1. Cybersecurity Is a priority.

- Eighty-one percent of advisers say that cybersecurity is high or very high among their firm's priorities.

2. There are gaps in both awareness and preparation.

- Fewer than half (44%) of respondents said they 'completely agree' that they fully understand the risks associate with cybersecurity.
- Only 26 percent of respondents say they 'completely agree' that they are fully aware of what would be required to adhere to the guidelines set out by the Office of Compliance Inspections and Examinations (OCIE).

3. Those gaps are perceived as bigger when respondents are asked about their teams

- Thirty-four percent of firm CEOs say they 'completely agree' that their teams fully understand the risks associate with cybersecurity.
- Eleven percent of firm CEOs say they 'completely agree' that their team is fully aware of what would be required to adhere to the guidelines set out by OCIE.

4. While many firms offer some form of training to close these gaps, it is not always mandatory.

- Fewer than half of firms (44%) with more than one team member provide mandatory training for employees.

In this paper we'll examine two aspects of preparing your team to understand and respond to cybersecurity risks. First we'll look at team structure. Specifically, we'll focus on how firms assign responsibility to oversee and execute on issues related to cybersecurity and if and how they find external support for that process. Next we'll look at team training and how firms are helping new and current employees understand the key issues on an on-going basis.



CYBERSECURITY: IS YOUR TEAM PREPARED?

Team Structure

Firms are investing an increasing amount of time in understanding, monitoring and responding to issues associated with cybersecurity. That increased commitment of time creates a clear challenge, as firms seek to assign responsibility for this complex issue to team members who are already busy. And while firms assign responsibility differently, only nine percent of firms say that the cybersecurity role is a dedicated role. For 91 percent of firms, the responsibility for cybersecurity is only one of several roles an individual may have.

According to respondents, responsibility for cybersecurity is an internal role. And while only five percent of firms say the responsibility lies with an external consultant, the firm is still accountable for the adequacy of the program offered by the consultant(s). More specifically, the CEO or CCO takes on overall responsibility for creating, implementing and monitoring policies and procedures related to cybersecurity.

However, the size of the firm plays an important role. The CEOs of firms generating less than \$250k in revenue will routinely take on this responsibility (62%), dropping to just eight percent for firms generating \$2.5m or more in revenue. As firms increase in size, responsibility shifts either to a CCO or another internal role.

The data highlights a particular challenge for the leaders of smaller firms who are taking on this critical role and who are, very likely, stretching their individual capacity. Once firms reach \$1m or more in annual revenue, they are more likely to have the ability to delegate responsibility to another senior team member.

Team Structure



Question: Who is primarily responsible for creating, implementing and monitoring policies and procedures related to cybersecurity on your team?

| WHO | ALL RESPONDANTS | LESS THAN \$250K | \$250K-\$499.9K | \$500K-\$999.9K | \$1M-\$2.49M | \$2.5M+ |
|--|-----------------|------------------|-----------------|-----------------|--------------|---------|
| The CIO | 7% | 4% | 4% | 6% | 6% | 9% |
| The CCO | 32% | 12% | 20% | 38% | 50% | 46% |
| The CEO | 33% | 62% | 43% | 35% | 13% | 8% |
| Another internal role (not CIO, CCO, or CEO) | 15% | 6% | 13% | 10% | 19% | 27% |
| An outside consultant | 5% | 3% | 7% | 7% | 8% | 5% |
| No one, other or I don't know | 8% | 12% | 12% | 4% | 3% | 4% |

Just as responsibility for oversight and execution vary by firm, so does the investment of time. While the majority of respondents indicated they invest less than 20 hours per year, there was a significant range across firms and by role. More than quarter of non-adviser management indicated they had invested more than 40 hours in dealing with cybersecurity issues in the last year. The investment is significant.

QUESTION: In the last year, how much time have you personally invested in understanding or managing the implementation of policies and procedures related to cyber-security?

| TIME | ALL RESPONDANTS | CEO | ADVISERS | NON-ADVISER MANAGEMENT | SUPPORT STAFF |
|--------------------|-----------------|-----|----------|------------------------|---------------|
| Less than 10 hours | 37% | 39% | 43% | 23% | 34% |
| 10-19 hours | 28% | 30% | 28% | 25% | 24% |
| 20-39 hours | 17% | 16% | 15% | 23% | 17% |
| 40 hours+ | 13% | 11% | 7% | 27% | 15% |



CYBERSECURITY: IS YOUR TEAM PREPARED?

Finding Support

The demands that are being placed on firms has caused many to seek outside help. Two-thirds of firms are using outside consultants to support them in implementing policies and procedures. Eighty-nine percent of the largest firms use external consultants in some way.

Question: Do you work with outside consultants and/or vendors to help you manage cybersecurity risks?

| | ALL RESPONDENTS | LESS THAN \$250K | \$250K-\$499.9K | \$500K-\$999.9K | \$1M-2.49M | \$2.5M+ |
|--------------|-----------------|------------------|-----------------|-----------------|------------|---------|
| Yes | 67% | 45% | 65% | 74% | 80% | 89% |
| No | 26% | 49% | 29% | 21% | 13% | 11% |
| I don't know | 7% | 5% | 6% | 5% | 7% | 0% |

For technical issues, firms who use external consultants are more likely to use them both to consult and execute (60%); only 19 percent use them purely on a consulting basis. For operational issues and for education and training, firms rely less on external consultants for implementation, but do tap into their expertise as consultants.

Question: With which aspects of cybersecurity do consultants help and what is the type of help provided? (n=those using outside consultants)

| FUNCTION | CONSULTING ONLY | IMPLEMENTATION ONLY | CONSULTING AND IMPLEMENTATION | I DON'T KNOW |
|------------------------|-----------------|---------------------|-------------------------------|--------------|
| Technical | 67% | 45% | 65% | 74% |
| Operational | 26% | 49% | 29% | 21% |
| Education and Training | 7% | 5% | 6% | 5% |

Education and training is typically delivered internally, even if the firm relies on the consulting services of an external resource.



CYBERSECURITY: IS YOUR TEAM PREPARED?

Finding Support

In general, formal training of any kind is a challenge for advisory firms, particularly for smaller firms with smaller teams. The **FPA 2015 Trends in Adviser Compensation and Benefits Study** highlighted the fact that even when firms offer team development, those activities are more likely to be informal (e.g., mentoring or training). Cybersecurity adds one more area that needs to be addressed, raising a question as to whether this training needs to be formal and/or mandatory.



On the following pages we'll share how advisers are addressing the key components of training including scope, frequency and content as we pose questions about your own training process. As you read about what your peers are doing, think about your own training process and if/how that needs to improve.



Finding Support

Sixty percent of respondents say their firm provides some form of cybersecurity training for new employees and 64 percent provide that training to current employees. Therefore, about a one-third of teams aren't receiving any training related to cybersecurity. With only 12 percent of respondents suggesting that training is the most challenging aspect of a cybersecurity plan, ensuring employees are properly trained should not be a matter of concern.

The training that is provided may or may not be mandatory. Larger firms are more likely to provide mandatory training for both new employees (49%) and current employees (57%). However, the smallest firms struggle to provide mandatory training (36 percent for new employees and 34 percent for current employees)

Question: Do you provide training, related to cybersecurity for new employees? (n=those with at least two team members)?

| | ALL RESPONDENTS | LESS THAN \$250K | \$250K-\$499.9K | \$500K-\$999.9K | \$1M-2.49M | \$2.5M+ |
|---|-----------------|------------------|-----------------|-----------------|------------|---------|
| Yes, we conduct a mandatory program | 44% | 36% | 44% | 44% | 44% | 49% |
| Yes, we conduct a non-mandatory program | 16% | 12% | 22% | 12% | 17% | 24% |

QUESTION: Do you provide training, related to cybersecurity for current employees?

| | ALL RESPONDENTS | LESS THAN \$250K | \$250K-\$499.9K | \$500K-\$999.9K | \$1M-2.49M | \$2.5M+ |
|---|-----------------|------------------|-----------------|-----------------|------------|---------|
| Yes, we conduct a mandatory program | 44% | 34% | 40% | 46% | 50% | 57% |
| Yes, we conduct a non-mandatory program | 20% | 16% | 27% | 17% | 21% | 24% |

Think about your business and the fact that the most successful businesses are more likely to make cybersecurity training mandatory. Do you need to make any changes? If you aren't sure, use your own clients as a litmus test. If a client asked you how you train your team to keep their data secure, would anything less than describing a mandatory training program feel adequate? How would your clients feel if you told them there was no training provided or that it was optional for team members?



CYBERSECURITY: IS YOUR TEAM PREPARED?

Finding Support

How much time does your team spend annually on cybersecurity training?

Today, the average team member receives less than two hours of cybersecurity training per year. Some firms provide considerably more with eleven percent of firms indicating their team members each receive five hours or more of training per year. The number of training hours appears to be more related to preference than to access to resources; larger firms do not necessarily expect additional hours of training.

Question: How many hours per year would a typical employee spend in training related to cybersecurity issues? (n=those who provide employee training)?

| TIME | ALL RESPONDENTS |
|----------------------|-----------------|
| Less than 60 minutes | 31% |
| 1-2 hours | 34% |
| 3-4 hours | 18% |
| 5-6 hours | 5% |
| 7 hours + | 6% |
| I don't know | 6% |

While a minority of firms (21%) provide one-time training, most who provide training make it an on-going process (79%). As with the number of hours provided, the decision to make training on-going is consistent across firms and not related to the size of the firm.

Think about your business and the amount of time that you feel is appropriate to be fully trained on the issues that are relevant for the team. Do you feel the amount of time your team invests in training is adequate? Beyond the number of hours, do you have a culture that reinforces a focus on security and data protection? Does the team see this reflected in the actions of the firm and the leadership? In the same way that firms now refer to creating 'culture of compliance' we may need to think about how the culture of the firm reinforces a focus on data protection.

Finding Support



How long are training sessions?

In general, firms try to keep individual training sessions to under 60 minutes (65%) with some stretching to two hours (22%). While a majority of the largest firms follow the same pattern, they are more likely to offer intensive training sessions with 18 percent providing training that lasts three hours or more for new employees. Training for current employees is generally under two hours.

QUESTION: How long is/was the one-time training program for employees? (n=those providing one-time training)?

| TIME | ALL RESPONDENTS | LESS THAN \$250K | \$250K-\$499.9K | \$500K-\$999.9K | \$1M-\$2.49M | \$2.5M+ |
|----------------------|-----------------|------------------|-----------------|-----------------|--------------|---------|
| Less than 60 minutes | 65% | 82% | 50% | 65% | 73% | 55% |
| 1-2 hours | 22% | 18% | 39% | 20% | 13% | 18% |
| 3-4 hours | 6% | 0% | 6% | 15% | 7% | 9% |
| 5 hours+ | 2% | 0% | 6% | 0% | 0% | 9% |
| I don't know | 4% | 0% | 0% | 0% | 7% | 9% |

QUESTION: How long is/was the on-going training program for employees? (n=those providing on-going training)?

| TIME | ALL RESPONDENTS | LESS THAN \$250K | \$250K-\$499.9K | \$500K-\$999.9K | \$1M-\$2.49M | \$2.5M+ |
|----------------------|-----------------|------------------|-----------------|-----------------|--------------|---------|
| Less than 60 minutes | 50% | 54% | 49% | 38% | 61% | 50% |
| 1-2 hours | 32% | 31% | 38% | 44% | 16% | 48% |
| 3-4 hours | 5% | 5% | 3% | 3% | 7% | 0% |
| 5 hours+ | 6% | 0% | 6% | 6% | 9% | 3% |
| I don't know | 8% | 10% | 6% | 9% | 7% | 0% |

Finding Support



*QUESTION: How long is an on-going session for current employees?
(n=those offering on-going training to current employees)*

| TIME | ALL RESPONDENTS | LESS THAN \$250K | \$250K-\$499.9K | \$500K-\$999.9K | \$1M-\$2.49M | \$2.5M+ |
|----------------------|-----------------|------------------|-----------------|-----------------|--------------|---------|
| Less than 60 minutes | 54% | 45% | 46% | 54% | 64% | 62% |
| 1-2 hours | 34% | 38% | 42% | 35% | 25% | 37% |
| 3-4 hours | 3% | 7% | 1% | 5% | 4% | 0% |
| 5 hours+ | 3% | 0% | 5% | 4% | 3% | 2% |
| I don't know | 5% | 10% | 5% | 2% | 4% | 0% |

Think about your own business and consider keeping training brief. The issues associated with cybersecurity are dense and complex. Team compliance is likely to increase when there is clarity; however, the average person has limits when it comes to how much information can be absorbed at one time. Consider your own training. Should you offer more frequent, but shorter sessions?

Finding Support



How often is your team being trained?

The frequency of training will most certainly be tied to the number of hours offered; however, there is a significant range across firms on this issue. The largest proportion of firms (38%) offer annual training, but there is no clear preference. The smallest firms offer more frequent (but potentially shorter) training sessions.

| FREQUENCY | ALL RESPONDENTS | LESS THAN \$250K | \$250K-\$499.9K | \$500K-\$999.9K | \$1M-\$2.49M | \$2.5M+ |
|---------------|-----------------|------------------|-----------------|-----------------|--------------|---------|
| Monthly | 9% | 10% | 9% | 11% | 9% | 8% |
| Quarterly | 19% | 29% | 13% | 22% | 13% | 24% |
| Semi-Annually | 12% | 7% | 15% | 12% | 16% | 14% |
| Annually | 38% | 29% | 36% | 31% | 41% | 43% |
| Other | 17% | 19% | 22% | 19% | 19% | 8% |
| I don't know | 6% | 7% | 5% | 5% | 3% | 4% |

Think about your own business. Once you have identified the appropriate number of hours for training and the optimal length of a meeting, the ideal frequency will emerge. As the data in the next section suggests, frequency may also be supported by using different formats to deliver training.

Finding Support



How do you deliver your training?

Training is typically delivered in person, but many firms are taking advantage of other forms of training with one-third offering on-line courses and nearly half sending e-mail alerts. As important, many firms are using multiple formats for their training rather than choosing one over the other. The majority of firms are covering all of the fundamental topics including:

- Policies and procedures
- The risks associated with cybersecurity
- The role of the team in mitigating risk

Question: What is the method of training provided? Please select all that apply. (n=those who provide employee training)

| METHOD | ALL RESPONDANTS | LESS THAN \$250K | \$250K-\$499.9K | \$500K-\$999.9K | \$1M-\$2.49M | \$2.5M+ |
|-----------------|-----------------|------------------|-----------------|-----------------|--------------|---------|
| In Person | 86% | 83% | 86% | 82% | 94% | 79% |
| On-line courses | 33% | 26% | 30% | 34% | 22% | 33% |
| Email alerts | 46% | 33% | 35% | 43% | 36% | 53% |
| Other | 7% | 7% | 5% | 11% | 8% | 2% |
| I don't know | 1% | 0% | 2% | 2% | 1% | 0% |

Think about your own business. Are you making use of training formats that not only create efficiencies, but drive engagement? Are you tapping into the preferred learning methods of your team?



CYBERSECURITY: IS YOUR TEAM PREPARED?

Steps to Take Action

The way in which you structure and train your team to mitigate the risks associated with cybersecurity will depend heavily on the size of the business. However, the following actions will help move you forward no matter the size of your team.



Steps to Take Action



1. Define clear goals with respect to cybersecurity

- a. There are clear and documented requirements set forth by OCIE both for the business and specifically for team training
Review and set goals to ensure you are able to meet those requirements.

2. Define your expectations of the team as it relates to those goals

- a. Clearly define what you expect of the team with respect to awareness, understanding or participation in the safeguarding of the business and your clients. Your expectations should be clear, actionable and easy to understand.

3. Gather input from the team

- a. Talk to the team about their questions or concerns related to cybersecurity to understand where they see potential risks and how they perceive their own level of knowledge or awareness.

4. Conduct an internal assessment anonymously

- a. Ask team members to rate their level of awareness and understanding on each of the requirements set forth by OCIE. Consider doing this anonymously as the goal is not to highlight any individual, but to understand where you need to focus your training efforts.
- b. Use the assessment provided in this whitepaper which outlines each of the elements of the OCIE requirements. Ask the following questions – either for each of the six overall areas of examination or for each individual component within those six areas.
 - i. Are you aware of this requirement? (Response: yes/no)
 - ii. Do you have any involvement in executing on this requirement? (Response: yes/no/I don't know)
 - iii. How would you rate your level of understanding of what is required to meet this requirement (Response: Scale of 1-5 from “do not understand at all” to “completely understand”)
 - iv. To the best of your knowledge, has the firm met this requirement? (Response: yes/no/I don't know)

Steps to Take Action



Actions Continued

5. Identify gaps

- a. On the basis of the team assessment, identify where you need to focus your training to close any potential gaps. Gaps may relate to general awareness/understanding, the role the team plays in taking action or the perception of where the firm is relative to executing on the requirements.

6. Create/refine and package your training process

- a. Create a clear, mandatory training program and ensure you have addressed each of the following:
 - i. Is the program mandatory or optional?
 - ii. Is the program offered to new employees, current employees or both?
 - iii. Is the program delivered on a one-time basis or an on-going basis?
 - iv. What is the total amount of training a team member should receive?
 - v. What is the frequency and length of the training sessions?
 - vi. How will you deliver the training?
 - vii. Will you deliver the training yourself or provide the team with access to external training resources?
 - viii. What are the topic areas you will cover?
 - ix. How will you measure the successful completion of the training program?

7. Create a summary of your training process

- a. Map out the training program and summarize it on a single page that you can share with clients or other partners. This communication will reinforce your commitment to safeguarding your clients in a way that is more formalized.

In the next whitepaper we'll go deeper into the details of what advisory firms are doing to safeguard their businesses. Specifically, we'll focus on the scope of breaches in the industry today and which tools, technology and processes firms are implementing to stay safe.



CYBERSECURITY: IS YOUR TEAM PREPARED?

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-ADVISED MANAGEMENT | 12% |
| SUPPORT 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 | 24% |
| Yes, I have overall responsibility and manage the execution of policies and | 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% |



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