FPA FINANCIAL PLANNING ASSOCIATION

RESEARCH & PRACTICE INSTITUTE™

Sponsored By

TD Ameritrade Institutional

CYBERSECURITY WHITEPAPER

Cybersecurity: Current Threats And Risk Management

CYBERSECURITY: CURRENT THREATS AND RISK MANAGEMENT

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 what their plans are going forward.

This is the third in a series of three whitepapers that will focus on the tactical issues associated with cybersecurity, including client communication, team training and risk management. In this whitepaper we'll share information on the threats advisers have faced and, more importantly, the technologies and processes they are putting in place to safeguard their clients and their businesses going forward. 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: CURRENT THREATS AND RISK MANAGEMENT

Scope of Risk

This report begins with the good news that a relatively small number of advisory firms report experiencing a firm or client-level security breach. Among the largest firms, eight percent report a breach, dropping to three percent among the smallest firms. However, a higher percentage of respondents weren't aware if there had been a security breach than reported having one, creating the potential that the actual number is higher. Larger firms are more likely to report that data has been compromised in the last 12 months, a trend we'll see throughout this report.

Question: Has any of your firm-level or client data ever been compromised as a result of a security breach?

	ALL RESPONDENTS	LESS THAN $250	$250K - $499.9K	$500K - $999.9K	$1M - $2.49M	$2.5M+
Yes	4%	3%	2%	4%	7%	8%
No	89%	92%	94%	91%	88%	86%
I don't know	7%	5%	4%	5%	4%	5%

Where breaches have occurred, the most common form of breach was hacking of client emails; however, other firms have experienced internal breaches and third-party vendor breaches.

Question: What type(s) of breach have you experienced? Please select all that apply. (n=those who have been breached)

	ALL RESPONDENTS
Internal network breach	16%
Third party vendor breach	28%
Client email was hacked	60%
Other	16%
I don't know	2%

Scope of Risk

On a related note, there is little agreement as to who should be contacted first in the case of a security breach. The largest proportion of respondents (46%) indicated they would contact their technology consultant, with one-third reaching out to their custodian or broker dealer.

Question: Who would you/your firm call first if a security breach was discovered?

	ALL RESPONDENTS	LESS THAN $250	$250K - $499.9K	$500K - $999.9K	$1M - $2.49M	$2.5M+
An attorney	8%	9%	9%	7%	10%	8%
SEC/ Regulators	4%	5%	3%	4%	2%	1%
Tech consultant/ expert	46%	35%	40%	44%	56%	69%
Custodian/ broker dealer	31%	39%	41%	38%	22%	18%
I don't know	12%	12`%	7%	7%	9%	4%

***BEST PRACTICE** – To save valuable time when a security breach occurs, create an "Incident Response Plan" of what should happen in the event of a security incident.*

Phishing attempts are less commonly understood or tracked. About one-third of firms do not know how many phishing attempts have occurred; however, a significant majority of the largest firms (66%) say there has been at least one documented occurrence in the last year. Once again, the largest firms appear to be the prime targets for phishing attempts, a similar pattern as was seen with security breaches. Ninety-three percent of the largest firms reported a recent phishing attempt.

Question: How many phishing attempts has your firm had in the past 12 months?

	ALL RESPONDENTS	LESS THAN $250	$250K - $499.9K	$500K - $999.9K	$1M - $2.49M	$2.5M+
None	25%	42%	33%	23%	19%	7%
1 to 3	17%	14%	17%	20%	24%	16%
4 to 6	8%	5%	6%	7%	11%	22%
7 or more	16%	9%	13%	15%	21%	28%
I don't know how many phishing attempts there have been	33%	29`%	31%	35%	25%	27%
I'm not familiar with the term "phishing attempt"	1%	1%	0%	1%	1%	0%

***BEST PRACTICE** – One of the easiest ways to limit the potential for a phishing attempt is to ensure your email systems are updated with all necessary patches and updates.*

CYBERSECURITY: CURRENT THREATS AND RISK MANAGEMENT

Monitoring Risk

While many respondents are taking steps to secure data, there is room for improvement as it relates to continuous monitoring. Just over half (56%) of all respondents indicated they had conducted a formal scan for vulnerabilities, increasing to 72 percent among the largest firms. Larger firms are more likely to use outside consultants for such scans.

Question: Have you conducted a formal scan for cybersecurity vulnerabilities in your business? Please select all that apply.

	ALL RESPONDENTS	LESS THAN $250K	$250K-$499.9K	$500K-$999.9K	$1M-$2.49M	$2.5M+
Yes, we conducted a scan internally	28%	30%	33%	24%	23%	27%
Yes, we used an outside firm to conduct a scan	28%	13%	21%	31%	39%	45%
No	35%	54%	43%	32%	29%	28%
I don’t know	16%	7%	10%	17%	15%	8%

CYBERSECURITY: CURRENT THREATS AND RISK MANAGEMENT

Monitoring Risk

Among those firms that have conducted a scan there is almost no agreement as to the appropriate frequency. For a small number of respondents (7%) the scan was a one-time activity although an additional 21 percent consider scans an on-going, but ad hoc, process.

Question: How frequently are scans completed?
(n=those who have completed a scan)

	ALL RESPONDENTS	LESS THAN $250K	$250K-$499.9K	$500K-$999.9K	$1M-$2.49M	$2.5M+
It was a one-time activity	7%	6%	7%	8%	3%	9%
As needed, but on no set schedule	21%	37%	22%	21%	20%	11%
Monthly	22%	31%	24%	22%	11%	17%
Quarterly	10%	8%	13%	3%	15%	17%
Semi-annually	3%	0%	3%	1%	3%	4%
Annually	14%	5%	6%	22%	18%	20%
Other	10%	7%	21%	8%	10%	2%
I don't know	14%	6%	4%	14%	20%	20%

***BEST PRACTICE** – Consider scanning for potential vulnerabilities more frequently. Your goal is to reduce the number of vulnerabilities over time and only scanning quarterly or annually leaves your systems open to potential attack.*

CYBERSECURITY: CURRENT THREATS AND RISK MANAGEMENT

Technology and Process

Respondents agree that cybersecurity poses a real risk, that tackling the issue is a priority and that there is work to be done. But there is less agreement as to how such plans should be executed with respondents using a range of technologies and processes to store, share and protect firm and client data. The approaches that are being used vary dramatically across all respondents and, in particular, between the smallest and largest firms.

CYBERSECURITY: CURRENT THREATS AND RISK MANAGEMENT

Data Storage

There is limited agreement on the safest way to store data. While approximately one-third of respondents (36%) indicate that cloud-based storage is most secure, a quarter of respondents feel data should be housed on a local server. There were limited differences in viewpoints based on the size of the firm.

WHERE IS YOUR DATA STORED?

Question: What do you consider the safest way to store your client's/firm's information?

	ALL RESPONDENTS
Cloud	36%
Local server	25%
Offsite server	12%
Any of the above is equally secure	15%
I don't know	12%

BEST PRACTICE *– The best way to secure sensitive data is to ensure you are doing the basics well, including understanding what is sensitive, setting rules for data types, ensuring it is being handled according to the rules, and educating your team on the rules.*

Data Storage

With a majority of employees using some form of mobile technology, there are significant differences regarding whether those devices are provided by the company or personally provided. The largest firms are more likely to make use of mobile technology of all forms, presumably to support communication across larger teams. A relatively higher percentage of respondents indicate that laptops, tablets and, in particular, cell phones are personally provided (28%, 36% and 49% respectively). Whether corporately or personally provided, almost all respondents (96%) report having anti-virus software installed on their computers.

Question: Are the electronic devices, used by employees, provided by the company or provided personally?

		ALL RESPONDENTS	LESS THAN $250K	$250K-$499.9K	$500K-$999.9K	$1M-$2.49M	$2.5M+
LAPTOPS	Company provided	54%	49%	48%	60%	55%	62%
	Personally provided	28%	28%	28%	23%	30%	30%
	Not Applicable	18%	23%	23%	17%	15%	8%
TABLETS	Company provided	25%	22%	28%	21%	32%	34%
	Personally provided	36%	25%	34%	37%	39%	46%
	Not Applicable	39%	53%	28%	42%	29%	20%
CELL PHONES	Company provided	25%	32%	29%	20%	23%	24%
	Personally provided	59%	46%	28%	68%	63%	75%
	Not Applicable	16%	22%	23%	11%	15%	1%

***BEST PRACTICE** – Mobile devices make it easy for employees to be connected at all times, but they open your business up to the potential for security breaches if the devices are stolen or misplaced. Ensure these devices have all necessary safeguards and have the data erased if the device is transferred to another user or put out of service.*

CYBERSECURITY: CURRENT THREATS AND RISK MANAGEMENT

Data Storage

A majority of firms have an inventory of electronic devices used by the team; however, nearly one-third of respondents (30%) do not.

Question: Have you created an inventory of all electronic devices used by your firm/team?

	ALL RESPONDENTS	LESS THAN $250	$250K - $499.9K	$500K - $999.9K	$1M - $2.49M	$2.5M+
Yes	61%	68%	67%	52%	62%	63%
No	30%	29%	32%	40%	34%	28%
I don't know	9%	3%	1%	8%	5%	8%

CYBERSECURITY: CURRENT THREATS AND RISK MANAGEMENT

Data Security

In order to understand how advisers are ensuring that data is secure, we examined the protocols for data access and encryption. Among respondents with teams that use mobile technology, the use of third-party software is the most common way to ensure secure access. The largest firms are more likely to use multiple protocols (predominantly Virtual Private Networks and third party software); however, nearly a quarter of the smallest firms have no security protocols in place.

Question: What security protocols are in place to protect your firm data and client information? Please select all that apply. (n=those with employees using mobile technology)

	ALL RESPONDENTS	LESS THAN $250	$250K - $499.9K	$500K - $999.9K	$1M - $2.49M	$2.5M+
VPN	44%	34%	41%	29%	55%	50%
Token	27%	16%	19%	26%	31%	38%
Third party software	61%	56%	68%	60%	62%	55%
Other	12%	10%	5%	8%	13%	21%
None of the above	14%	22%	14%	19%	6%	12%

***BEST PRACTICE** – Only company provided hardware and devices should be able to connect to your company network – with or without the use of a Virtual Private Network (VPN) – and be sure users of the devices and hardware do not have administrator-level rights.*

Data Security

As it relates to logging-in to applications to access confidential data there are a range of measures being used to secure data with complex passwords dominating at 70 percent.

QUESTION: Which, if any, of the following do you require to log-in to applications that provide access to confidential client or firm information? Please select all that apply.

	ALL RESPONDENTS	LESS THAN $250K	$250K-$499.9K	$500K-$999.9K	$1M-$2.49M	$2.5M+
Simple password	13%	14%	17%	14%	11%	14%
Complex password	70%	67%	76%	71%	74%	76%
Two-factor authentication	39%	36%	34%	35%	44%	44%
Single sign on	20%	15%	22%	25%	12%	20%
Other	2%	3%	0%	1%	5%	4%
I don't know	6%	6%	3%	7%	5%	4%

As they relate to data encryption, the results are relatively positive, with nearly half of firms encrypting data both at rest and in transit. Once again, the smallest firms highlight greater potential risk with 21 percent of respondents indicating they do not encrypt data at all.

QUESTION: Do you encrypt your client data?

	ALL RESPONDENTS	LESS THAN $250K	$250K-$499.9K	$500K-$999.9K	$1M-$2.49M	$2.5M+
Yes, at rest only	6%	8%	7%	7%	4%	7%
Yes, in transit only	27%	21%	31%	26%	35%	34%
Yes, at rest and in transit	44%	42%	47%	43%	46%	44%
No	11%	21%	8%	11%	5%	8%
I don't know	11%	8%	8%	13%	11%	7%

***BEST PRACTICE** – When sensitive data is sent via email or other forms of distribution, it is open to potential attack unless it is encrypted properly. Review your company's type of data and determine which forms of data must be encrypted so it cannot be intercepted and used in fraudulent ways.*

Data Security

The need for data encryption is underscored by the fact that nearly half of respondents indicate that they receive confidential information from clients via email. What is clear from the data is that there is no one way that respondents receive confidential client information, which may be received by fax, secure email or mail. Almost all respondents indicated that multiple methods were used.

QUESTION: How do clients send confidential information to you? Please select all that apply.

	ALL RESPONDENTS	LESS THAN $250K	$250K-$499.9K	$500K-$999.9K	$1M-$2.49M	$2.5M+
Fax	62%	42%	65%	78%	69%	66%
Secure email	53%	47%	54%	53%	62%	59%
Email	49%	46%	49%	55%	53%	45%
Direct mail	72%	65%	72%	77%	69%	70%
In person	82%	76%	79%	91%	84%	80%
Secure online portal	51%	41%	50%	57%	56%	61%
Other	3%	6%	2%	4%	0%	0%

When distribution requests are received by clients, 91 percent of respondents indicated they verify the request by phone with nearly 20 percent also following up with an email. Two percent of firms indicated they do not confirm initial distribution requests.

As it relates to email, the vast majority of respondents indicated that personal emails are not used to conduct business; however, there are some exceptions. Fourteen percent of the smallest firms use personal emails for business – dropping to just three percent for the largest firms.

QUESTION: Does anyone use personal email to conduct business?

	ALL RESPONDENTS	LESS THAN $250K	$250K-$499.9K	$500K-$999.9K	$1M-$2.49M	$2.5M+
Yes	8%	14%	11%	7%	4%	3%
No	87%	84%	88%	90%	89%	92%
I don’t know	5%	2%	1%	3%	7%	6%

***BEST PRACTICE** – Personal email accounts should only be used for personal email correspondence and not for business. Create a policy that restricts employee use of personal email for business-related matters and strictly enforce it.*

CYBERSECURITY: CURRENT THREATS AND RISK MANAGEMENT

The Cost of Security

According to the experts, advisory firms can make significant strides toward a more secure environment with a limited budget, but costs can increase significantly for larger firms. Nearly half of the smallest firms say they have not invested anything on external or internal resources.

Question: 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?

	ALL RESPONDENTS	LESS THAN $250	$250K - $499.9K	$500K - $999.9K	$1M - $2.49M	$2.5M+
We have not invested externally	23%	48%	25%	16%	10%	5%
Less than $5,000	37%	41%	50%	48%	37%	23%
$5,000 - $9,999	12%	4%	13%	12%	23%	28%
$10,000 - $14,999	4%	0%	2%	5%	4%	14%
$15,000+	6%	1%	1%	2%	9%	11%
I don't know	19%	5%	9%	16%	17%	19%

Question: 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?

	ALL RESPONDENTS	LESS THAN $250	$250K - $499.9K	$500K - $999.9K	$1M - $2.49M	$2.5M+
We have not invested internally	21%	46%	21%	12%	11%	12%
Less than $5,000	44%	46%	61%	61%	42%	30%
$5,000 - $9,999	8%	3%	9%	4%	20%	20%
$10,000 - $14,999	3%	0%	1%	2%	3%	8%
$15,000+	5%	0%	0%	4%	7%	14%
I don't know	19%	3%	8%	18%	17%	16%

CYBERSECURITY: CURRENT THREATS AND RISK MANAGEMENT

The Cost of Security

The data highlights the range of technologies, processes and protocols being used to secure firm and client data. The range reflects preference or budgets, but best practices suggest a more secure path forward. Below is a summary of the best practices highlighted throughout this report, which can serve as an action plan for mitigating and managing risk in your business.

Review these best practices with your team and develop formal policies to protect you and your clients:

1. To save valuable time when a security breach occurs, **create an “Incident Response Plan”** of what should happen in the event of a security incident.

2. One of the easiest ways to limit the potential for a phishing attempt is to **ensure your email systems are updated with all necessary patches and updates.**

3. Consider **scanning for potential vulnerabilities more frequently.** Your goal is to reduce the number of vulnerabilities over time and only scanning quarterly or annually leaves your systems open to potential attack.

4. The best way to secure sensitive data is to **confirm you are doing the basics well,** including understanding what is sensitive, setting rules for data types, ensuring it is being handled according to the rules, and educating your team on the rules.

5. Mobile devices make it easy for employees to be connected at all times, but they open your business up to the potential for security breaches if the devices are stolen or misplaced. **Ensure these devices have all necessary safeguards and have the data erased** if the device is transferred to another user or put out of service.

6. **Only company provided hardware and devices should be able to connect to your company network** – with or without the use of a Virtual Private Network (VPN) – and be sure users of the devices and hardware do not have administrator-level rights.

7. When sensitive data is sent via email or other forms of distribution, it is open to potential attack unless it is encrypted properly. Review your company’s data types and **determine which forms of data must be encrypted** so it cannot be intercepted and used in fraudulent ways.

8. Personal email accounts should only be used for personal email correspondence and not for business. **Create a policy that restricts employee use of personal email for business-related matters and strictly enforce it.**

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-Adviser 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 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

CYBERSECURITY WHITEPAPER

Cybersecurity: Current Threats And Risk Management