Compilation of Results of a Pilot Survey of Cybersecurity Practices of Small and Mid-Sized Investment Adviser Firms

North American Securities Administrators Association
www.nasaa.org
About NASAA

Organized in 1919, the North American Securities Administrators Association (“NASAA”) is the oldest international organization devoted to investor protection. NASAA is a voluntary association with a membership consisting of securities administrators in the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Canada and Mexico.

State and provincial securities regulators have been protecting investors from fraud and abusive sales practices since the passage of the first “blue sky” law in Kansas in 1911 and since 1912 in Canada when Manitoba became the first province to approve securities legislation. In the United States, state securities regulation preceded federal securities laws, including the creation of the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), formerly the NASD.

As the preeminent organization of securities regulators, NASAA is committed to protecting investors from fraud and abuse, educating investors, supporting capital formation, and helping ensure the integrity and efficiency of financial markets.
A Pilot Survey To Compile Cybersecurity Information

Introduction: Developing A Pilot Cybersecurity Project

NASAA’s pilot cybersecurity project was designed to better understand the cybersecurity practices of state-registered investment advisers, which account for over half of the registered investment advisers conducting business in the United States. Through the use of a template survey, the pilot project sought to elicit information to better understand the technology and data practices of state-registered investment advisers; how these advisers communicate with clients; and what types of policies and procedures these advisers currently maintain. The pilot project also focused on specific uses of technology and websites, with a goal of understanding the safeguards used by state-registered investment advisers to protect client information; to inform state examination programs; and to identify national cybersecurity trends relevant to state-registered investment advisers.

States participating in the pilot project used the survey as part of their examinations and audit inspection programs or as a separate survey or document request tool. The survey allowed states participating in the pilot program to collect information on either an identifiable or anonymous basis. Some states sent the survey to a limited number of investment advisers registered in their states while others sent it to all of the investment advisers registered in their states. About half of the survey responses collected were collected on an anonymous basis initially, while the remainder were collected in an identifiable setting, whether through examinations or a document request. Several states also made the optional request that investment advisers submit relevant policies and

---

1 About one percent of investment registrants are registered with both the SEC and the states.
procedures. Nine states reported a subset of the investment adviser firms’ responses to NASAA on a non-identifiable basis.

Pilot Project Survey Results:
A Compilation of Data from 440 Registered Investment Advisers in 9 States

This subset of data includes 440 state-registered investment adviser firms of varying sizes. Forty-seven percent have assets under management of less than $25 million, thirty-seven percent manage more than $25 million, and sixteen percent do not manage assets. The firms have between 1 and 100 employees and between 1 and 39 investment adviser representatives. The firms average three employees and two investment adviser representatives.

State securities regulators are continuing to review the survey data, but note the following preliminary findings:

- Only 4.1% of firms indicated they had experienced a cybersecurity incident and even fewer, only 1.1%, indicated they had experienced theft, loss, unauthorized exposure, or unauthorized use of or access to confidential information.

- Most state-registered investment advisers (85%) use computers, tablets, smartphones, or other electronic devices to access client information.

- While 92% of firms use e-mail to contact clients, only 50% of the firms use secure e-mail. Furthermore, 56.7% of firms have procedures in place to authenticate instructions received from their clients via e-mail.

---

2 All surveyed firms are state registered.
• 62% of firms report undergoing a cybersecurity risk assessment. The frequency of these assessments varied widely.

• Just under one half of firms (44.4%) report having policies and procedures or training in place related to cybersecurity. Similarly, 47.5% of firms report having policies and procedures or training related to the disposal of electronic data storage devices. A total of 76.8% of firms reported maintaining policies and procedures related to technology or cybersecurity.3

Beyond Pilot Survey Results: Continuing the Regulatory Conversation on Cybersecurity

As state regulators continue to review the data, NASAA is now releasing the compilation of the pilot survey results to further inform regulatory and industry conversations on cybersecurity. Additional jurisdictions are administering the template survey, which will further enrich the ongoing regulatory conversations on cybersecurity. NASAA plans to continue to work with the jurisdictions that were pilot participants as well as additional jurisdictions to further analyze how cybersecurity developments affect state-registered investment advisers. Despite the relatively low rate in cybersecurity incidents identified in the compilation of pilot results, state securities regulators are aware of the increase in cyber-attacks in the financial services industry, and the importance and associated difficulties of securely maintaining private data.4

As NASAA’s study of cybersecurity practices of state-registered investment advisers continues, NASAA expects to begin working toward recommended practices and engage in additional conversation with industry.

For more information, please contact:

A.Valerie Mirko
Deputy General Counsel
NASAA
Email: vm@nasaa.org

Andrew Hartnett
Missouri Commissioner of Securities
& Chair of NASAA’s Investment Adviser
Cybersecurity & Technology Project Group
Email: andrew.hartnett@sos.mo.gov

NASAA Legal Department
750 First Street, NE, Suite 1140
Washington, DC 20002
202 737 0900

Missouri Secretary of State’s Office
600 W Main St.
Jefferson City, MO  65101
573 751 4136

3 The pilot project cybersecurity survey elicited information regarding a wide array of policies and procedures or training programs relating to technology, including cybersecurity, disposal of electronic data storage devices, use of social media, and other related topics. Please see page 13 for a full list.

Preliminary Survey Results:

Expenses Directly Related to Information Technology Security

Maintenance of the Firm’s Information Technology Systems

Rate of Cybersecurity Incidents

Client Contact via E-mail & Use of Secure E-mail

Authentication of Client Instructions Received Electronically

Devices Used to Access Client Information

Unauthorized Use or Access to Customer Information

Risk Assessments Related to Cybersecurity & Frequency of Risk Assessments

Insurance Coverage for Cybersecurity

Confidentiality Agreements with Third Party Service Providers with Access to Firm IT Systems

Policies, Procedures and Training Programs

Authentication Practices

Use of Antivirus Software

Antivirus Software Installed on Electronic Devices Used to Access Client Information

Frequency of Antivirus Updates

Use of Encryption

Use of On-Line or Remote Backup of Electronic Files

Use of Remote Access to Servers or Workstations via VPN or Similar Technology & Dual Factor Authentication

Patch Updates / Software Updates

Use of Free Cloud Services

Use of Software as a Service (“SAAS”) Vendors

Use of Mobile Device Management (“MDM”) Tools

Use of Firm Websites to Access Client Data

Use of Client Portals on Firm Websites

Use of SSL or Other Encryption on Website’s Client Portal
Expenses Directly Related to Information Technology Security

During the firm’s last fiscal year, what percentage of the firm’s overall expenses was directly related to information technology security?

- Not sure of firm’s overall expenses: 15%
- < 1% of firm’s overall expenses: 33%
- 1-3% of firm’s overall expenses: 33%
- 3-5% of firm’s overall expenses: 11%
- > 5% of firm’s overall expenses: 8%

Maintenance of the Firm’s Information Technology Systems

Who is responsible for the maintenance of the firm’s information technology systems?

- Employees: 34%
- External vendors: 9%
- Both: 58%
- Not sure: 15%
Rate of Cybersecurity Incidents

Has the firm experienced a cybersecurity incident during its registration in the jurisdiction in which it is registered?

- Yes: 4%
- No: 96%
Client Contact via E-mail & Use of Secure E-mail

Does your firm contact clients via e-mail or other electronic messaging?

- Yes: 92%
- No: 7%
- Not sure: 1%
- No response: 1%

If yes, does your firm use secure email?

- Yes: 54%
- No: 30%
- Not sure: 14%
- No response: 2%
Authentication of Client Instructions Received Electronically

Does your firm use any procedures to authenticate client instructions received via email/electronic messaging?

- Yes: 57%
- No: 13%
- Not applicable to my firm's business model: 29%
- No response: 1%

Devices Used to Access Client Information

Does your firm use computers, tablets, smartphones, or other electronic devices to access client information other than e-mail/electronic messaging?

- Yes: 85%
- No: 14%
- No response: 1%
Unauthorized Use or Access to Customer Information

Has your firm, directly or indirectly, experienced theft, loss, unauthorized exposure, or unauthorized use of or access to customer information?

- Yes: 1%
- No response: 6%
- No: 93%
Risk Assessments Related to Cybersecurity & Frequency of Risk Assessments

Does your firm conduct risk assessments to identify cybersecurity threats, vulnerabilities, and potential consequences?

- Yes: 62%
- No: 37%
- No response: 1%

If yes, how often does your firm conduct risk assessments to identify cybersecurity threats, vulnerabilities, and potential consequences?

- Annually: 40%
- Quarterly: 13%
- Monthly: 11%
- Weekly: 10%
- Other: 25%
- No response: 1%
Insurance Coverage for Cybersecurity

Does your firm maintain any insurance coverage for cybersecurity?

- Yes: 17%
- No: 67%
- Not applicable to firm's business model: 14%
- No response: 2%

Confidentiality Agreements with Third Party Service Providers With Access to Firm IT Systems

Does your firm have confidentiality agreements with any third party service providers (i.e., custodians, sub-advisers, etc.) with access to your firm’s information technology systems?

- Yes: 43%
- No: 23%
- Not applicable to firm's business model: 32%
- No response: 2%
### Policies, Procedures and Training Programs

**Does your firm have policies and procedures or training programs in place regarding any of the following?**

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td>44.6%</td>
</tr>
<tr>
<td>The disposal of electronic data storage devices</td>
<td>47.4%</td>
</tr>
<tr>
<td>Detecting unauthorized activity on your networks or devices</td>
<td>38.0%</td>
</tr>
<tr>
<td>Your firm’s continued operation during a cyber-event or cyber security incident</td>
<td>39.6%</td>
</tr>
<tr>
<td>Oversight of your firm’s third-party information technology or data service providers (e.g. vetting, contract with service provider or vendor, confidentiality requirements)</td>
<td>38.0%</td>
</tr>
<tr>
<td>Loss of electronic devices (e.g. loss of a laptop containing personal and confidential client information)</td>
<td>39.2%</td>
</tr>
<tr>
<td>Accessing client communications or client information from a device not dedicated to business usage (e.g. home laptop, public computer at an airport)</td>
<td>41.5%</td>
</tr>
<tr>
<td>Relating to the use of social media for business purposes (e.g. Linkedin, Twitter, Facebook, other)</td>
<td>50.9%</td>
</tr>
<tr>
<td>Other technology issues not listed above</td>
<td>13.4%</td>
</tr>
<tr>
<td>None - my firm has no policies and procedures regarding any of the above</td>
<td>23.1%</td>
</tr>
</tbody>
</table>

---

5 This question required that respondents check all categories that applied.
What forms of authentication are required by customers or employees to access electronic data storage devices, which allow access to client communications and/or client information?

- **No authentication required**: 3.7%
- **Single factor authentication (e.g., ID/Password)**: 73.3%
- **Dual factor authentication (e.g., Key FOBS, secure IDs)**: 41.1%
- **Adaptive factor authentication (Challenge questions)**: 21.5%
- **Biometric authentication (e.g., fingerprint scan)**: 4.8%
- **Other authentication**:
  - 2.5%
- **No response**: 3.2%
Use of Antivirus Software

Does your firm utilize antivirus software?

Yes: 97%
No: 2%
No response: 1%

Antivirus Software Installed on Electronic Devices Used to Access Client Information

If yes, is the antivirus software installed on all computers, tablets, smartphones, or other electronic devices used to access client information?

Yes: 87%
No: 10%
No response: 3%
All firms that reported utilizing antivirus software reported that such software is updated periodically.

*All firms that reported utilizing antivirus software reported that such software is updated periodically.*
Use of Encryption

Does your firm utilize encryption on its files or devices?

- Yes: 39%
- No: 46%
- Not sure: 13%
- No response: 2%

If yes, is the encryption software required on all computers, tablets, smartphones, or other electronic devices used to access client information?

- Yes: 60%
- No: 32%
- No Response: 4%
- Not Sure: 4%
Use of On-Line or Remote Backup of Electronic Files

Does your firm utilize on-line or remote backup of electronic files?

- Yes: 76%
- No: 22%
- No response: 2%
**Use of Remote Access to Servers or Workstations via VPN or Similar Technology & Dual Factor Authentication**

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>No response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does your firm allow remote access to servers or workstations via a virtual private network (VPN) or similar technology?</td>
<td>73%</td>
<td>64%</td>
<td>3%</td>
</tr>
<tr>
<td>If yes, do you require dual factor (e.g., Key FOBS, secure IDs) authentication for access?</td>
<td>24%</td>
<td>73%</td>
<td>3%</td>
</tr>
</tbody>
</table>
Patch Updates / Software Updates

How does your firm patch (update software on) all laptop or tablet computers, or other portable electronic devices, such as smartphones?

- Automatically by vendor (Windows update, Java update, Adobe, etc.) 73%
- Manually 9%
- Not sure 9%
- Patch management software 3%
- No response 6%

Manually 9%
Use of Free Cloud Services

Does your firm use free Cloud services such as iCloud, Dropbox or Google Drive, to store personal and confidential client information?

- Yes: 17%
- No: 82%
- No response: 1%

If yes, is there a policy that stipulates how these services are to be used?

- Yes: 44%
- No: 53%
- No response: 3%
Use of Software as a Service (SAAS) Vendors

If your firm uses Software As A Service (SAAS) vendors for application development, do you vet the vendor for security issues?

- Yes 20%
- No 32%
- No response 48%

Use of Mobile Device Management (MDM) Tools

Does your firm utilize a Mobile Device Management (MDM) tool (e.g., Airwatch, MobileIron, Citrix/XenMobile)?

- No 85%
- Yes 4%
- Not sure 6%
- No response 5%
Use of Firm Websites to Access Client Data

Does your firm utilize your firm’s website to use or access client information data?

- Yes: 7%
- No: 66%
- N/A Firm does not have a website: 25%
- No response: 2%

If yes, do you use SSL or other encryption?

- Yes: 77%
- Not sure: 13%
- No: 10%
Use of Client Portals on Firm Websites

Does your firm’s website include a client portal?
- Yes: 18%
- No: 51%
- N/A Firm does not have a website: 24%
- No response: 7%

Use of SSL or Other Encryption on Website’s Client Portal

If yes, do you use SSL or other encryption?
- Yes: 74%
- Not sure: 13%
- No: 10%
- No response: 3%