Cybersecurity Practices of Ohio Investment Advisers; A Summary of Survey Responses

October 2014
A Pilot Survey to Compile Cybersecurity Information

In July 2014, the Ohio Division of Securities participated in the North American Securities Administrators Association’s (“NASAA”) pilot cybersecurity project. For this project, NASAA worked with state securities regulators to utilize a template survey sent to state-licensed investment advisers in order to elicit information about the technology and data practices of that registrant population. A compilation of results of NASAA’s survey can be found at: www.nasaa.org/industry-resources/investment-advisers/nasaa-cybersecurity-report/.

For its effort, the Ohio Division of Securities surveyed over 500 Ohio-domiciled, state-licensed investment advisers. This report summarizes the 266 responses received. The Division thanks our investment adviser community for dedicating their time and insight to provide thorough, thoughtful, and timely responses. The Division also thanks NASAA for its support in conducting and compiling this important survey.

Ohio Pilot Project Survey Results:

- Only 3% of responding firms indicated they had experienced a cybersecurity incident and even fewer, less than 1%, indicated they had experienced theft, loss, unauthorized exposure, or unauthorized use of, or access to, confidential information.

- The majority of responding firms (87%) use computers, tablets, smartphones, or other electronic devices to access client information.

- 88.9% of responding firms use e-mail to contact clients. Only 54% of those firms, however, use secure e-mail.

- Of those that use e-mail to contact clients, 45% of responding firms have procedures in place to authenticate instructions received from their clients electronically.

- 62% of responding firms report undergoing a cybersecurity risk assessment. The frequency of these assessments varied widely.

- Less than half of responding firms (40%) report having policies and procedures or training in place related to cybersecurity. Similarly, 44% of responding firms report having policies and procedures or training related to the disposal of electronic data storage devices. Only one third of reporting firms (32%) have policies, procedures, or training programs designed to detect unauthorized activity on their networks or devices.
Survey Results

AUM Breakdown for Surveyed Firms

- More than $25 million AUM, 35%
- Under $25 million AUM, 47%
- No AUM or not provided, 18%
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?

- < 1% of firm's overall expenses: 33%
- 1-3% of firm's overall expenses: 28%
- 3-5% of firm's overall expenses: 10%
- > 5% of firm's overall expenses: 9%
- Not sure of firm's overall expenses: 20%

Maintenance of the Firm’s Information Technology Systems

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

- Employees: 31%
- External Vendors: 9%
- Both: 60%

During the Firm's last fiscal year, what percentage of the firm's overall expenses was directly related to information technology security?
Rate of Cybersecurity Incidents

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

- Yes, 3%
- No, 97%
Client Contact via Email & Use of Secure E-mail

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

- Yes, 89%
- No, 10%
- No Response, 1%

If yes, does your firm use secure email?

- Yes, 54%
- No, 31%
- Not sure, 15%
Authentication of Client Instructions Received Electronically

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

- Yes, 45%
- No, 15%
- Not applicable to my firm's business model, 39%
- 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 email/electronic messaging?

- Yes, 87%
- No, 13%
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, 0.8%
No, 99.2%
Risk Assessments Related to Cybersecurity & Frequency 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, 8%
- Monthly, 9%
- Weekly, 12%
- Other, 20%
- No response, 11%
Insurance Coverage for Cybersecurity

Does your firm maintain any insurance coverage for cybersecurity

- No, 58%
- Yes, 20%
- Not applicable to firm's business model, 18%
- No response, 4%

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?

- No, 21%
- Yes, 42%
- Not applicable to firm's business model, 34%
- No response, 3%
Policies, Procedures, and Training Programs

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

- Cybersecurity
- The disposal of electronic data storage devices
- Detecting unauthorized activity on your networks or devices
- Your firm's continued operation during a cyber-event or cyber security incident
- Oversight of your firm's third-party information technology or data service providers (e.g., vetting, contract with service provider or vendor, confidentiality requirements)
- Loss of electronic devices (e.g., loss of a laptop containing personal and confidential information)
- Accessing client communications or client information from a device not dedicated to business usage (e.g., home laptop, public computer at an airport)
- Relating to the use of social media for business purposes (e.g., LinkedIn, Twitter, Facebook, other)
- Other technology issues not listed above
- None - my firm has no policies and procedures regarding any of the above

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

- **Single factor authentication** (e.g., ID/password): 70%
- **Dual factor authentication** (e.g., Key FOBS, secure IDs): 32%
- **Adaptive factor authentication** (Challenge questions): 27%
- **Biometric authentication** (e.g., fingerprint scan): 3%
- **Other authentication**: 6%
- **No response**: 3%
- **No authentication is required**: 5%

Note: this question required that respondents check all categories that applied.
Use of Antivirus Software

Does your firm utilize antivirus software?

- Yes, 98%
- No, 1%
- No response, 1%

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

- Yes, 88%
- No, 10%
- No response, 2%
Frequency of Antivirus Updates

How often are updates downloaded to antivirus software?

- Automatically, 84%
- Weekly, 3%
- Annually, 3%
- Monthly, 1.6%
- Quarterly, 0.4%
- No response, 2%
- Other, 2%
- Not sure, 4%
Use of Encryption

Does your firm utilize encryption on its files or devices?

- Yes, 38%
- No, 43%
- Not sure, 17%
- 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, 38%
- Not sure, 2%
Use of Online or Remote Backup of Electronic Files

Does your firm utilize online or remote backup of electronic files?

- Yes, 70%
- No, 28%
- No response, 2%
Use of Remote Access to Servers or Workstations via VPN or Similar Technology & Dual Factor Authentication

Does your firm allow remote access to servers or workstations via a virtual private network (VPN) or similar technology?

- Yes, 26%
- No, 71%
- No response, 3%

If yes, do you require dual factor (e.g., Key FOBS, secure IDs) authentication for access?

- Yes, 64%
- No, 36%
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.), 58%
- Manually, 11%
- Not sure, 24%
- No response, 6%
- Patch management software, 1%
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, 20%
- No, 79%
- No response, 1%

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

- Yes, 23%
- No, 77%
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?

- No, 40%
- Yes, 16%
- No response, 44%
- Not sure, 4%

Use of Mobile Device Management (MDM) Tools

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

- No, 76%
- Yes, 4%
- Not sure, 15%
- No response, 4%
Use of Firm Websites to Access Client Data

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

- Yes, 5%
- No response, 3%
- N/A Firm does not have a website, 22%
- No, 70%

If yes, do you use SSL or other encryption?

- Yes, 67%
- No, 33%
Use of Client Portals on Firm Websites

Does your firm's website include a client portal?

- Yes, 13%
- N/A Firm does not have a website, 24%
- No response, 4%
- No, 59%

If yes, do you use SSL or other encryption?

- Yes, 66%
- Not sure, 24%
- No, 10%