CYBERSECURITY SURVEY FOR DELAWARE REGISTERED INVESTMENT ADVISERS

Introduction

You are receiving this cybersecurity survey because your firm is an Investment Adviser registered with the State of Delaware. The Investor Protection Unit for the Delaware Department of Justice is seeking your assistance to help us identify best practices when it comes to cybersecurity issues.

In order to carry out their duties, investment advisers usually handle client information of a personal and confidential nature which must be done in a careful and prudent manner. The issue of cybersecurity has become increasingly prevalent. There has been extensive media coverage of the latest cyber-attack by hackers as well as regulatory interest in this subject from the SEC, FINRA, state securities regulators, and financial services regulators generally.

The Investor Protection Unit is asking for your assistance in completing the survey below. This information will help us determine whether the significant issues of cybersecurity are addressed by investment adviser registrants and, if those issues are remaining unaddressed, whether investment adviser firms seek guidance in this area. We are also interested in understanding existing good practices which can help regulators in providing guidance in this area.

Please be advised that the Investor Protection Unit plans on implementing the cybersecurity request for information as part of their routine examination/regulatory process starting in January 2015.

The results of this survey may be shared with other state securities regulators who are conducting similar initiatives, so that we may identify best practices across the industry. If you have any concerns about such sharing, please call the Investor Protection hotline at (302) 577-8424 so that your concerns may be addressed.

Please fill out this request for information in its entirety and mail your responses back to the address listed below by **Friday, October 31, 2014**.

Thank you very much for your assistance.

Instructions/Glossary

For purposes of this survey, the terms "*you*", "*your*" or "*firm*" mean the recipient's Delaware-registered investment adviser firm. For purposes of this survey, the term "*related person*" includes any and all of the firm's officers, partners, directors, employees, or any person performing similar functions.

Identifying Information

Firm Name:

Firm IARD Number:

Contact Person:

Has your firm experienced one or more cybersecurity incident(s)?

No ◯

Yes ◯

If so, state when this occurred and describe the general nature of the incident(s).

Firm Information

Does your firm have assets under management?

◯ Yes ◯ No

If yes, please indicate whether you manage:

◯ Under $25 million AUM

◯ More than $25 million AUM

Number of employees (include non-registered employees):

Number of investment adviser representatives:

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

◯ < 1% ◯ 1-3% ◯ 3-5% ◯ > 5% ◯ Not sure

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

◯ Employees ◯ External vendors ◯ Both

Has your firm experienced a cybersecurity incident during its registration in Delaware?

◯ Yes ◯ No

Questions

General Questions

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

◯ Yes ◯ No

If yes, does your firm use secure email?

◯ Yes ◯ No ◯ Not sure

(2) Does your firm use any procedures to authenticate instructions received from clients via e-mail or other electronic messaging?

◯ Yes ◯ No ◯ Not applicable to my firm's business model

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

◯ Yes ◯ No

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

◯ Yes ◯ No

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

◯ Yes ◯ No

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

◯ Weekly

◯ Monthly

◯ Quarterly

◯ Annually

◯ Other

(6) Does your firm maintain any insurance coverage for cybersecurity?

◯ Yes ◯ No ◯ Not applicable to my firm's business model

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

◯ Yes ◯ No ◯ Not applicable to my firm's business model

Policies/Procedures & Training

(8) Does your firm have policies and procedures or training programs in place regarding any of the following: (please check all that apply)

☐ 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 client 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

Accessing Electronic Information

(9) 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 (includes all computers, tablets, smartphones, or other electronic devices). Please select all that apply:

☐ No authentication is required

☐ Single factor authentication (e.g. ID/ Password)

☐ Dual factor authentication (e.g. Key FOBS, secure IDs)

☐ Adaptive factor authentication (Challenge questions)

☐ Biometric authentication (e.g. fingerprint scan)

☐ Other authentication

(10) Does your firm utilize antivirus software?

◯ Yes ◯ No

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

◯ Yes ◯ No

How often are updates downloaded to the antivirus software?

◯ Not sure

◯ Automatically

◯ Never

◯ Weekly

◯ Monthly

◯ Quarterly

◯ Annually

◯ Other

(11) Does your firm utilize encryption on its files or devices?

◯ Yes ◯ No ◯ Not sure

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

◯ Yes ◯ No ◯ Not sure

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

◯ Yes ◯ No

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

◯ Yes ◯ No

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

◯ Yes ◯ No

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

◯ Manually

◯ Automatically by vendor (Windows update, Java update, Adobe, etc.)

◯ Patch management software

◯ Not sure

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

◯ Yes ◯ No

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

◯ Yes ◯ No

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

◯ Yes ◯ No

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

◯ Yes ◯ No ◯ Not sure

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

◯ Yes ◯ No ◯ N/A My firm does not have a website

If yes do you use SSL or other encryption.

◯ Yes ◯ No ◯ Not sure

(19) Does your firm's website include a client portal?

◯ Yes ◯ No ◯ N/A My firm does not have a website

If yes do you use SSL or other encryption.

◯ Yes ◯ No ◯ Not sure

(20) Provide a copy your firm's policies and procedures as they relate to cybersecurity and protection of client information. Please either cut and paste a copy of your firm's policies and procedures in the text box below or send it as an attachment with the completed survey. Thank you