Cybersecurity Plan

11/15/2016

APPLETON GROUP, LLC

INVESTMENT SOLUTIONS · WEALTH MANAGEMENT
EMPLOYER-SPONSORED PLANS

Table of Contents

Summary

The Securities and Exchange Commissions (SEC) came out with a risk alert on Cybersecurity in April 2014. The risk alert contains 28 detailed questions, seeking information pertaining to the cybersecurity controls and practices used in the firm. The information requested includes the following categories:

- Identification of risks/cybersecurity governance
- Protection of firm networks and information
- Risks associated with remote customer access and funds transfer requests
- Risks associated with vendors and other third parties
- Detection of unauthorized activity
- Other

The SEC has clearly indicated that firms will be required to respond to these information requests and that there will be a certain standard that RIA firms will need to adhere. Appleton Group, LLC recognizes the importance of having a reasonably secure office environment that protects the confidential information of our clients. Therefore, we have designed this Cybersecurity Plan to address the security and protection of all non-public information.

Definitions

The following words and phrases used throughout this document have the following meanings:

Personal Information - Personal information is defined as a client's first and last name or first initial and last name and one or more of the following: 1) social security number, 2) driver's license number or state-issue identification number, 3) any financial account number, including credit/debit card number or bank account number. Personal information does not include publicly available information or information legally obtained from federal, state, or local government records.

Security Breach – the unauthorized, acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a client.

Encrypted – the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key.

Record(s) – any material upon which written, drawn, spoken, visual or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Objectives

The objective of the Cybersecurity Plan is to:

1. Ensure the security and confidentiality of client information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information;
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any client.

The Plan shall provide standards and procedures for the protection of client privacy and security of our internal computer systems. Each employee will be required to review this plan and attend training to understand their responsibility. The standards and procedures will incorporate our current computer inventory and configurations, client data sources and service provider information as supporting documentation for this plan.

The Plan will incorporate the following items:

- Identify – this section provides our understanding of what the cybersecurity risks are to our systems, assets, data and capabilities.
- Protect- this area details the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – take action regarding a detected cybersecurity event.
- Recover – develop and implement the appropriate activities to maintain plans to recover and restore any services that were impaired due to a cybersecurity event.

Within each of the above items there are categories and subcategories of activities that need to be completed to insure that an adequate amount of protection and security is provided. Exhibit A provides more detail regarding above items.

Program Components

In order to develop and/or maintain an effective cybersecurity program, there are certain components that are necessary. Based on guidance from the SEC, following are specific areas that are covered in this plan:

- Risk Assessment – This assessment covers the type of client and proprietary information we maintain. In addition, the assessment includes an inventory of all hardware, software, email systems, anti-viral protection, firewalls, web based application, remote access tools and security authentication protocols. Furthermore, the assessment includes an inventory of our third-party vendors and what type of access they may have to our client and proprietary information. Finally an analysis is prepared periodically to gauge how effective our current systems are to handle a breach or any cybersecurity incidents. The analysis will include a recommendation on what or if any actions should be taken to provide a more secure environment for our clients.

- Policies and Procedures – Once the risk assessment has been developed, written policies and procedures must be implemented or updated. These policies and procedures will cover the following:
    - Roles and Responsibilities of employees, affiliates and third-party vendors
    - Accessibility of client and proprietary information
    - Security Protections of client and proprietary information
    - Monitoring, Identifying and Responding to Breaches
    - Vendor Oversight
    - Insurance that can help protect clients and our firm
    - Identify Theft protection and responding to attacks
    - Disaster Recovery from a cybercrime
    - Testing effectiveness of cybersecurity program

Responsibilities

Appleton Group, LCC shall designate the Chief Compliance Officer as the person responsible for maintaining the Cybersecurity Plan. This person shall be responsible for:

1. Identifying foreseeable and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of client information and systems that store client information.
2. Assessing the likelihood and potential damage of these threats:
3. Assessing the sufficiency of policies, procedures, client information systems, and other arrangements in place to control risks. In addition, when deficiencies are detected, make the appropriate recommendations to management in order to correct such deficiencies.
4. Test and monitor the effectiveness of key controls, systems and procedures.
5. Train staff to implement the cybersecurity program.
6. Oversee service providers which includes selecting and retaining service providers capable of maintaining appropriate safeguards of client information and require service providers to implement and maintain safeguards.
7. Evaluate and adjust the cybersecurity program to reflect results from testing and monitoring relevant technology changes, material changes to operations and business arrangements and any other circumstance that may have a material impact on the program.
8. Report any data security breach to the specific compliance regulators according to the procedures for responding to incidents or unauthorized access or use of personal information.

Client Data Information Systems Inventory

There are a number of client records that are kept in electronic and/or paper document format. A list of the systems where these records are kept is in Exhibit A. Since 2002 client documents haven been stored electronically on a computer server. Original signature paper documents are stored in locked filing cabinets. In addition, there are books and records stored in locked filing cabinets (tax returns, paid client invoices, employee documents….). Lastly, we have AGPLX mutual fund client information stored offsite through USBank Fund Services.

Cybersecurity Framework

An assessment of potential risk is made to determine if there are any potential gaps in current procedures and policies. A matrix of this assessment is on Exhibit B. The assessment includes risks to exposure of client information and the procedures and/or policies that exist to reasonably halt any possible intrusion.

Security Breach

Our firm's policy is to respond to a breach by safeguarding employees' lives and firm property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the firm's books and records, and allowing our client to transact business. If a security breach occurs, the Chief Compliance Officer and Chief Executive Officer with the assistance of StrataDefense, will be responsible for identifying what information was breached and the cause for the breach. The Chief Compliance Officer and the Chief Executive Officer will also notify the following parties about the information leak and update procedures and policies to remedy the problem:

- Employees
- Law enforcement
- Regulators, including any states that require notification
- Clients affected
- Insurer
- Other parties as appropriate

Threat Awareness Program

Because of the constantly changing and increasing sophistication of computer hackers, it is becoming more likely that computer hackers may successfully breach or compromise our information systems. One of the best techniques to address this concern is to incorporate best practices from other firms to help in combating any potential intrusion. We will constantly update a list of resources and firms that can provide techniques and procedures to incorporate in this Cybersecurity Plan that will help mitigate any potential breach into our computer systems. We will use these perceived threats to update the risk matrix (Exhibit B) and incorporate best practices to help reduce the risk.

Training

All employees are required to be trained annually on the security information program. As part of this training, employees will be updated with changes in the program including policies and procedures. Employees will also be required to update their passwords for the various points of access to personal client information.

Monitoring and Testing

The security information program will be monitored on an on-going basis. This includes monitoring of computer systems to confirm there are no unauthorized access and/or use of client personal information. In addition, physical office procedures will also be monitored to confirm there is no unauthorized access to the office space. The security information program will be tested annually to confirm policies and procedures are working appropriately. The Chief Compliance Officer will lead the testing process and evaluate if any changes are necessitated based on test results.

Remote Access

Remote access to individual computer workstations is allowed. The 2 layer remote access software allows employees to log on their computer workstations securely. Employees may access confidential client information via this secure connection, but may not download documents with client information onto their personal computers. Any employees who telecommute must access the information in the same manner. Employees may not transfer and download client personal information to their personal computers.

Disciplinary Measures

Employees are required to follow the procedures and policies in this security information program. Any employee who violates any procedure or policy will be subject to disciplinary action

Terminated Employee Access

Any terminated employee who previously had access to client personal information will be deactivated in our systems. This includes office keys, user ids and passwords to our computer system and programs and remote access to custodian websites.

Third-Party Service Providers

We have certain third-party service providers that may have access to client personal information. These are listed in Exhibit C. All third-party service providers have been notified that they must adhere to the requirements of our security information program. As part of this requirement, all service providers are required to submit a certification form that indicates they will adhere to the requirement of this plan

Client Data Access

All client personal information requested is to help in servicing the client or to address requirements from custodian we work with or regulatory agencies. The SEC requires we keep client information for the duration of the client relationship and at a minimum of 5 years. Only current employees are allowed access to client information and only if they require it for the purpose of servicing the client. In addition, a client's financial advisor is also allowed access to the client personal information and only for the purpose of servicing the client

GENERAL INFORMATION SECURITY STANDARDS

The following general security standards apply to all employees and affiliates. These standards encompass all aspects of our organization that affects security. This includes computer security, physical security and personnel procedures:

- All employees are required to have a unique user id and password that will be assigned to them for their workstation. Employees are not permitted to provide their password to other employees or any other non-employee unless authorized by the CCO.
- Keys to the office are authorized for employees only.
- Segregation of duties and double-checks of client information entry is required in operational tasks.
- Computer systems are protected by hardware firewall that helps to detect potential intrusion.
- In the event of unauthorized intrusion, we will investigate and provide feedback to the client and authorities.
- Client data is backed up nightly on-site and a removable portable tape is securely stored offsite daily.
- Computer workstations require a user id and password to access the server stored in a locked closet. The computer server also requires a user id and password. Access to this server is limited to StrataDefense our IT provider, and their approved employees. All passwords must consist of at least 14 characters.
- All user ids and passwords will be kept in a password protected file only accessible by the Chief Compliance Officer and anybody he or she designates.

PHYSICAL SECURITY STANDARDS

- Client information shall not be left unattended in offices or conferences rooms.
- Client files, documents, or other records shall be stored in locked cabinets or locked desks/bureaus when not in use and at the end of the day.
- Visitors are not allowed to walk unescorted in areas where client information is accessible.
- All records or documents containing client information shall be destroyed or shredded and thrown away in a secure container.
- Office should be locked at end of the day and access to offices during off-business hours is restricted to employees and cleaning crew only. Authorization to allow non-employees during non-business hours must be approved.
- The last employee in the office at night is responsible to make sure all computer workstations and filing cabinets are securely locked.

ELECTRONIC RECORDS SECURITY STANDARDS

- Workstations should be locked when left unattended for a significant amount of time. In addition, screen savers should be turned on to incorporate password protection.
- Password protection for access to workstations, laptops and computer servers is mandatory and will be changed periodically. Employees should not divulge their password and not store them where others can access them.
- Client data is backed up daily to an on-site a Highly Reliable brand back up system. The portable drive is encrypted and taken home nightly where it is securely stored. Annually, data on the off-site server is downloaded to test the back-up system. Access to the off-site server and portable hard drive is restricted to authorized personnel only.
- Access to client data on the firm's network system is available only to employees who require access to service the client or to conduct firm operations.
- Access to client data through various channels is controlled by the Chief Compliance Officer. There is a process set up to monitor access of client data when employees are hired and terminated.
- Monitoring of access to electronic documents containing client personal information will be performed by the Chief Compliance Officer on an on-going basis.

CONTINGENCY AND DISASTER SECURITY STANDARDS

- A disaster recovery plan is implemented and tested annually to confirm access to client data from offsite location and communication is available to clients, financial advisors and employees.
- Client data is stored on-site and backed up on a portable tape taken home nightly. Third party vendors with client data can be accessed through the cloud as well.
- A contingent location is identified in the disaster recovery plan and is equipped to function as an office for the time period needed until the primary office location is available or another location has been identified. All existing security standards implemented in the primary office location will be implemented in the contingent office location as well.

COMPUTER SYSTEM SECURITY REQUIREMENTS

- The Chief Compliance Officer will be responsible for the distribution of user ids and passwords for the various computer programs and website accounts that house client personal information.
- All current user ids and passwords will be stored in a password protected file that is available only to the Chief Compliance Officer and any other person that the CCO designates
- Access to all program and online websites that require user ids and passwords are only available to current employees.
- All online custodial websites where client personal information is available blocks users who have unsuccessfully attempted to log on. All computer workstations that have access to personal client information and are blocked from access if a sufficient number of unsuccessful attempts have been made.
- Access to records containing client personal information is only provided to employees who require it to service the client's account.
- Email encryption software is installed on all computer workstations. Employees are required to encrypt emails containing client personal information or use the secure portal.
- Certain employees also remotely log into the company server workstations. In these cases, secure remote software is used to access office computers. Any client personal information accessed is encrypted while connected to the office computer.

EXHIBIT A: CLIENT DATA INFORMATION SYSTEMS INVENTORY

Type of System	Location	Type of documents
File Cabinets	Storage Room	Paper client documents and books and records of firm
Computer Server	Locked IT Closet	Stores electronic documents containing client personal information.
Computer Workstation	Office	Has access to electronic documents containing client personal information
Computer Workstation	Office	Has access to electronic documents containing client personal information
Computer Workstation	Office	Has access to electronic documents containing client personal information
Computer Workstation	Office	Has access to electronic documents containing client personal information
Computer Workstation	Office	Has access to electronic documents containing client personal information
Computer Workstation	Office	Has access to electronic documents containing client personal information
Computer Workstation	Office	Has access to electronic documents containing client personal information
Computer Workstation	Office	Has access to electronic documents containing client personal information
Computer Workstation	Office	Has access to electronic documents containing client personal information
2 Computer Laptops	Traveling	Has access to electronic documents containing client personal information
Computer Laptop	Conference Room 1 and Conference Room 2	Has access to electronic documents containing client personal information
Desks, Bookshelves and Bureaus	Various Offices	Paper documents kept in binders and folders containing client personal information
Back Up Drive	Hooked to Server	Electronic documents containing client personal information
Backup Portable Hard Drive	Secured stored at Chief Compliance Officer home nightly	Encrypted electronic documents containing personal information

EXHIBIT B: CLIENT INFORMATION RISK MATRIX

Risk	Level of Risk	Controls	Gaps & Response
Access to electronic client information via a workstations or server	Low	All workstations including the server require a user id & password for access	Passwords could be guessed and access could be granted. Employees are required to use at least 14 character passwords
Laptop computer left in plain view	Medium	Laptop computers require a user id and password for access	Passwords could be guessed and access could be granted. Passwords are changed periodically
Filing cabinet left unlocked	High	Filing cabinets are required to be locked at the end of each day	Operations personnel may forget to lock cabinets at night. Employees are required to confirm cabinets are locked after use
Client folders & documents left out in public view	Medium	Client documentation is required to be put away at the end of the day	Employees may forget to put away client documents. Employees are required to confirm that any client documents are put away in a drawer or filing cabinet before leaving for the day
Employees discuss client personal information with unauthorized person	Low	Employees are required to confirm with the client if okay to divulge information to a third party who enquires about their personal information	Employees may not confirm with the client regarding if okay to release personal information
Employees do not lock workstation and close programs that have client data	Medium	Employees are required to close out all programs that have client data and lock their workstations	Employees may fail to lock their workstation. Employees are required to confirm that computers are locked before leaving for the day or to lunch

Client documents not thrown away in secure bin	Low	Employees are required to throw documents with client information in the secure bin	Employees may throw away documents with client information in a trash can. Employees are required to throw any client documents in the secure container
Client information emailed to client or authorized third-party without password or encryption	Medium	Employees are requested to fax information to third-party or client as an alternative to encrypting emails	Employees may not password protect documents and could be opened by an unauthorized party. Employees are required to encrypt emails when sending client documents.
Server is not protected from intrusion via the internet	Medium	Server is protected with firewall hardware which protects from internet intrusion	Firewall hardware fails due to mechanical or hacker attack. An intrusion is annually performed by an outside computer consultant
Office door is left open	Low	Employees are required to lock door if last to leave office	Employees forget to lock door before leaving the office
Laptop is left at a public place	Medium	Employees should always be aware of location of laptop. Security software installed on laptop. Requires user id and password	Employees may leave a laptop at public location and could be stolen or left behind. Security software can shut down laptop and make it inoperable

EXHIBIT C: THIRD PARTY SERVICE PROVIDER LIST

Name	Address	Service Provided
Charles Schwab, Inc.	211 Main Street San Francisco, CA 94105	Custodian for client assets
StrataDefense	8400 Highland Drive Wausau, WI 54401	IT provider
Pension, Inc.	1980 Commercial Way Green Bay, WI 54311	TPA/Recordkeeper for managed 401(k) plans
Fiduciary Partners	3913 W Prospect Ave Ste 201 Appleton, WI 54914	Trust company for managed client accounts
Wipfli	469 Security Blvd Green Bay, WI 54313	TPA/Recordkeeper for managed 401(k) plans
Midatlantic	1251 Waterfront Place Pittsburgh, PA 15222	Custodian for 401(k) client assets
Morningstar Office	22 W Washington Street Chicago, WI 60602	Client relationship manager system
Baker Tilly VK	205 N Michigan Avenue Chicago, IL 60601	Accountant
Pfefferle Management	200 E Washington St Ste 2A Appleton WI 54911	Landlord and housekeeping vendor
Cuna Mutual		

BEST PRACTICES LIST OF CONTACTS

Charles Schwab

Cuna Mutual

StrataDefense

RIA Compliance

Investment News

Pat Doyle-Attorney

Webinars