North American Securities Administrators Association

Cybersecurity Checklist for Investment Advisers

Identify Protect Detect Respond Recover

Identify: Risk Assessments & Management	YES	NO	N/A
1. Cybersecurity is included in the risk assessment.			
2. Risk assessments are conducted frequently. (e.g. annually, quarterly)			
3. The risk assessment includes an examination of the data its business collects and creates, where it is stored, and whether or not it is encrypted.			
4. Internal "insider" risk (e.g. disgruntled employees) and external risks are included in the risk assessment.			
5. The risk assessment includes relationships with third parties.			
6. Adequate policies and procedures demonstrate expectations of employees regarding cybersecurity practices (e.g. frequent password changes, locking of devices, reporting of lost or stolen devices, etc.).			
7. Primary and secondary person(s) are assigned as the central point of contact in the event of a cybersecurity incident.			
8. Specific roles and responsibilities are tasked to the primary and secondary person(s) regarding a cybersecurity incident.			
9. The firm has an inventory of all hardware and software.			
Protect: Use of Electronic Mail	YES	NO	N/A
1. Identifiable information of a client is transmitted via email.			

2. Authentication practices for access to email on all devices (computer and mobile devices) is required.			
3. Passwords for access to email are changed frequently (e.g. monthly, quarterly).			
4. Policies and procedures detail how to authenticate client instructions received via email.			
5. Email communications are secured. (If the response is no, proceed to the next question.)			
6. Employees and clients are aware that email communication is not secured.			
Protect: Devices	YES	NO	N/A
1. Device access (physical and digital) is permitted for authorized users, including personnel and clients.			
2. Device access is routinely audited and updated appropriately.			
3. Devices are routinely backed up and underlying data is stored in a separate location (i.e. on an external drive, in the cloud, etc.)			
4. Backups are routinely tested.			
5. The firm has written policies and procedures regarding destruction of electronic data and physical documents.			
6. Destruction of electronic data and physical documents are destroyed in accordance with written policies and procedures.			
Protect: Use of Cloud Services	YES	NO	N/A
1. Due diligence has been conducted on the cloud service provider prior to signing an agreement or contract.			
2. As part of the due diligence, the firm has evaluated whether the cloud service provider has safeguards against breaches and a documented process in the event of breaches.			

3. The firm has a business relationship with the cloud service provider and has the contact information for that entity.			
4. The firm is aware of the assignability terms of the contract.			
5. The firm understands how the its data is segregated from other entities' data within the cloud service.			
6. The firm is familiar with the restoration procedures in the event of a breach or loss of data stored through the cloud service.			
7. The firm has written policies and procedures in the event that the cloud service provider is purchased, closed, or otherwise unable to be accessed.			
8. The firm solely relies on free cloud storage.			
9. The firm has a back-up of all records off-site.			
10. Data containing sensitive or personally identifiable information is stored through a cloud service.			
11. Data containing sensitive or personally identifiable information, which is stored through a cloud service, is encrypted.			
12. The firm has written policies and procedures related to the use of mobile devices by staff who access data in the cloud.			
13. The cloud service provider (or its staff) has unfettered access to the firm's data stored in the cloud.			
14. The firm allows remote access to its network (e.g. through use of VPN).			
15. The VPN access of employees is monitored.			
16. The firm has written policies and procedures related to the termination of VPN access when an employee resigns or is terminated.			
Protect: Use of Firm Websites	YES	NO	N/A
1. The firm relies on a parent or affiliated company for the construction and maintenance of the website.			

2. The firm relies on internal personnel for the construction and maintenance of the website.			
3. The firm relies on a third-party vendor for the construction and maintenance of the website.			
4. If the firm relies on a third party for website maintenance, there is an agreement with the third party regarding the services and the confidentiality of information.			
5. The firm can directly make changes to the website.			
6. The firm can directly access the domain renewal information and the security certificate information.			
7. The firm's website is used to access client information.			
8. SSL or other encryption is used when accessing client information on the firm's website.			
9. The firm's website includes a client portal.			
10. SSL or other encryption is used when accessing a client portal.			
11. When accessing the client portal, user authentication credentials (i.e., user name and password) are encrypted.			
12. Additional authentication credentials (i.e., challenge questions, etc.) are required when accessing the client portal from an unfamiliar network or computer.			
13. The firm has written policies and procedures related to a denial of service issue.			
Protect: Custodians & Other Third-Party Vendors	YES	NO	N/A
1. The firm's due diligence on third parties includes cybersecurity as a component.			
2. The firm has requested vendors to complete a cybersecurity questionnaire, with a focus on issues of liability sharing and whether vendors have policies and procedures based on industry standards.			
3. The firm understands that the vendor has IT staff or outsources some of its functions.			

4. The firm has obtained a written attestation from the vendor that it uses software to ensure customer data is protected.			
5. The firm has inquired whether a vendor performs a cybersecurity risk assessment or audit on a regular basis.			
6. The cyber-security terms of the agreement with an outside vendor are <u>not</u> voided because of the actions of an employee of the firm.			
7. Confidentiality agreements are signed by the firm and third-party vendors.			
8. The firm has been provided enough information to assess the cybersecurity practices of any third-party vendors.			
9. [Relevant to custodians only] The firm has discussed with the custodian matters regarding impersonation of clients and authentication of client orders.			
Protect: Encryption	YES	NO	N/A
1. The firm routinely consults with an IT professional knowledgeable in cybersecurity.			
2. The firm has written policies and procedures in place to categorize data as either confidential or non-confidential.			
3. The firm has written policies and procedures in place to address data security and/or encryption requirements.			
4. The firm has written policies and procedures in place to address the physical security of confidential data and systems containing confidential data (i.e., servers, laptops, tablets, removable media, etc.).			
5. The firm utilizes encryption on all data systems that contain (or access) confidential information.			
6. The identities and credentials for authorized users monitored.			
Detect: Anti-Virus Protection and Firewalls	YES	NO	N/A
1. The firm regularly use anti-virus software on all devices accessing the firm's network, including mobile phones.			

2. The firm understands how the anti-virus software deploys and how to handle alerts.			
3. Anti-virus updates are run on a regular and continuous basis.			
4. All software is scheduled to update.			
5. Employees are trained and educated on the basic function of anti-virus programs and how to report potential malicious events.			
6. If the alerts are set up by an outside vendor, there is an ongoing relationship between the vendor and the firm to ensure continuity and updates.			
7. A firewall is employed and configured to appropriate to the firm's needs.			
8. The firm has policies and procedures to address flagged network events.			
Respond: Responding to a Cyber Event	YES	NO	N/A
1. The firm has a plan and procedure for immediately notifying authorities in the case of a disaster or security incident.			
2. The plans and procedures identify which authorities should be contacted based on the type of incident and who should be responsible for initiating those contacts.			
3. The firm has a communications plan, which identifies who will speak to the public/press in the case of an incident and how internal communications will be managed.			
4. The communications plan identifies the process for notifying clients.			
Recover: Cyber-insurance	YES	NO	N/A
1. The firm has considered whether cyber-insurance is necessary or appropriate.			
2. The firm has evaluated the coverage in a cybersecurity insurance policy to determine whether it covers breaches, including: breaches by foreign cyber intruders; insider breaches (e.g. legal expenses, notification expenses, third-party remediation expenses).			

3. The cybersecurity insurance policy covers notification (clients and regulators) costs.			
4. The firm has evaluated whether the policy includes first-party coverage (e.g. damages associated with theft, data loss, hacking and denial of service attacks) or third-party coverage (e.g. legal expenses, notification expenses, third-party remediation expenses).			
5. The exclusions of the cybersecurity insurance policy are appropriate for the firm's business model.			
6. The firm has put into place all safeguards necessary to ensure that the cybersecurity policy is not voided through the firm's employee actions, such as negligent computer security where software patches and updates are not installed in a timely manner.			
Recover: Disaster Recovery	YES	NO	N/A
1. The firm has a business continuity plan to implement in the event of a cybersecurity event.			
2. The firm has a process for retrieving backed up data and archival copies of information.			
3. The firm has written policies and procedures for employees regarding the storage and archival of information.			
4. The firm provides training on the recovery process.			