

# North American Securities Administrators Association

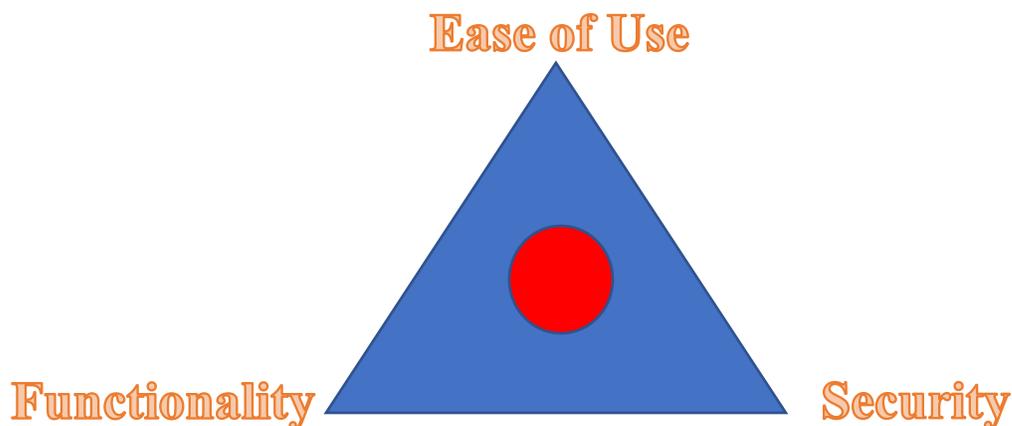
## Cybersecurity Checklist for Investment Advisers

### **Checklist Overview:**

The NASAA Model Rule and corresponding [Cybersecurity Checklist for Investment Advisers](#) are designed to assist firms in securing their systems and the non-public information of their clients. This guidance is designed to assist firms in better understanding the meaning, intention, and connectivity of each of the sections of the NASAA Cybersecurity Checklist for Investment Advisers.

The importance of cybersecurity is consistently illustrated through the nearly daily occurrence of large-scale data breaches. As such, NASAA proactively created this guidance to assist firms in addressing cybersecurity risks, securing their information technology infrastructure, identifying the occurrence of a risk event, confronting a cybersecurity incident, and, then, quickly normalizing business operations.<sup>1</sup>

To illustrate the importance of a balanced approach to cybersecurity, consider a common practice used by IT professionals known as the “Cybersecurity Triangle.” As pictured below, the goal of any cybersecurity procedure is to appropriately balance confidentiality, integrity, and availability. For example, one would not want client PII so available for business use that it is no longer confidential, but one also would not want it so secure that it is more secure than the nuclear football. Thus, the “Cybersecurity triangle” assists in illustrating the balance required by information technology procedures.



To ensure a cybersecurity procedure appropriately balances this approach, one must ensure that it is in the center of this triangle (i.e. the red circle). Thus, after completing the NASAA Cybersecurity Checklist for Investment Advisers, the firm should use the “Cybersecurity Triangle” as guidance when addressing any identified deficiencies.

---

<sup>1</sup> [NIST Framework](#)

\*All photographs were obtained from pexels.com.

## **Identify – Risk Assessments & Management**

1. Cybersecurity is included in the risk assessment.

If the firm does conduct an evaluation of its vulnerabilities, does the assessment include cybersecurity vulnerabilities that the firm possess.

2. Risk assessments are conducted frequently (e.g. annually, quarterly).

Does the firm conduct a frequent evaluation of the threats to which it is vulnerable?

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.

Is the firm's evaluation of its vulnerabilities granular enough to address specific types of data and the level to which it is secured?

4. Internal "insider" risk (e.g. disgruntled employees) and external risks are included in the risk assessment.

Does the firm have policies and procedures to address malicious employees and data extrication? Does the firm have policies and procedures to address the termination of employees and ensure their access to networks and data is restricted before or after their departure? Does the firm explore external risks related to the acts of clients, visitors, or maintenance staff?

5. The risk assessment includes relationships with third parties.

Does the firm's evaluation of its vulnerabilities address any third parties with whom it has executed agreements? If so, what due diligence does the firm conduct prior to executing such an agreement and continuously throughout the relationship?

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.)

Does the firm ensure that its employees are explicitly aware of their roles and responsibilities concerning cybersecurity? Are the firm's employees aware of the consequences for violating firm cybersecurity policies? Does the firm document the on-going education of its employees and instances of employee violations?

7. Primary and secondary person(s) are assigned as the central point of contact in the event of a cybersecurity incident.

Does the firm have designated individual(s) to handle cybersecurity incidents that occur? The firm should test its procedures as it develops to ensure that they are functioning prior to the actual occurrence of an incident.

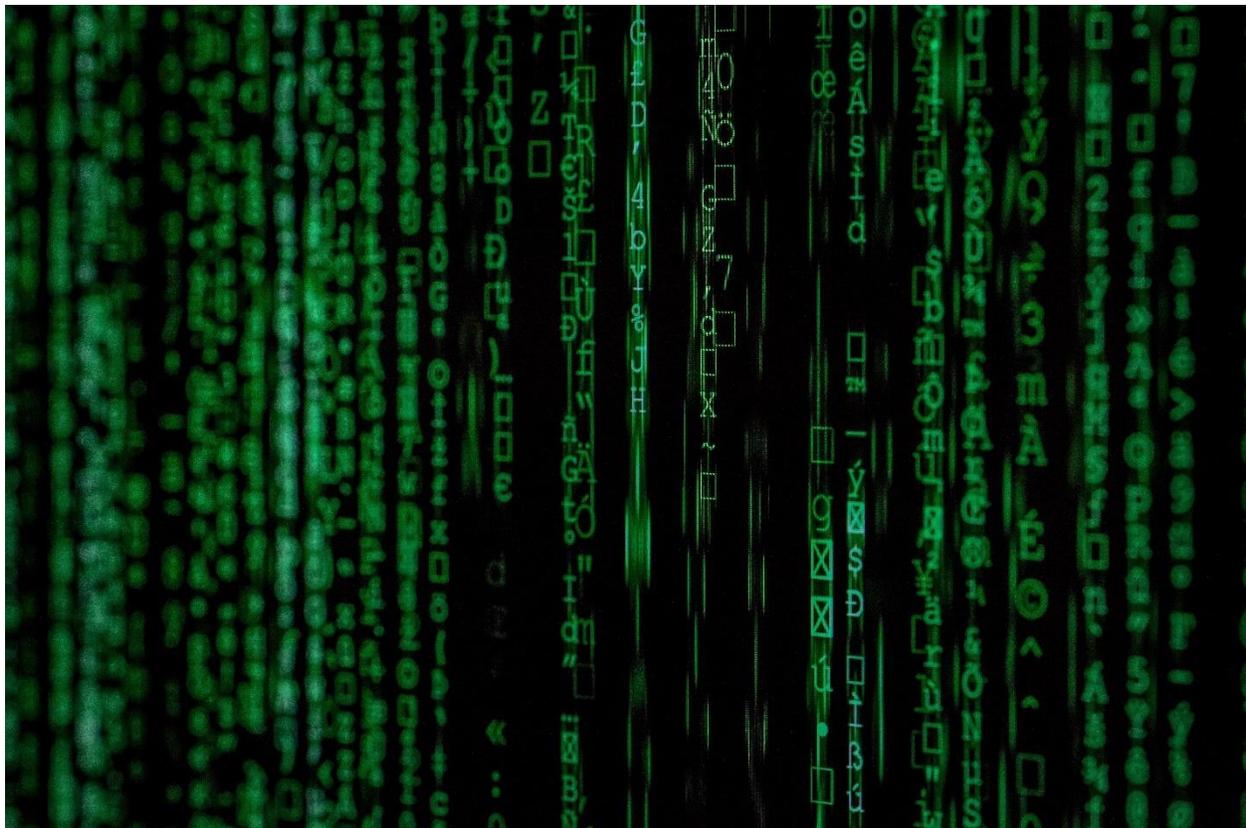


8. Specific roles and responsibilities are tasked to the primary and secondary person(s) regarding a cybersecurity incident.

Does the firm have specific responsibilities assigned to specific employees to ensure incidents are handled effectively and efficiently? The firm should ensure that the assigned roles and responsibilities have “back-ups” for the critical functions to ensure that, in the event a primary individual is unable to perform the assigned functions, the roles are still adequately performed.

9. The firm has an inventory of all hardware and software.

Is the firm able to quickly and accurately report the location of all its devices? Can the firm account for all software authorized to run on its network? These are essential to ensure that the firm can identify when unauthorized devices or programs access its digital assets.



## Protect – Use of Electronic Mail

1. Identifiable information of a client is transmitted via email

Does the firm electronically communicate non-public information of clients? If so, what safeguards does the firm have in place to protect this information?

2. Authentication practices for access to email on all devices (computer and mobile devices) is required.

What procedures does the firm have in place to ensure only authorized users are accessing the firm's electronic assets? Does the firm require encryption on all portable electronic devices? Does the firm require a passcode on all firm cell phones?

3. Passwords for access to email are changed frequently (e.g. monthly, quarterly).

What is the firm's password policy? Does the firm require a certain length and complexity be maintained in user passwords? How often are users required to update their passwords?

4. Policies and procedures detail how to authenticate client instructions received via email.

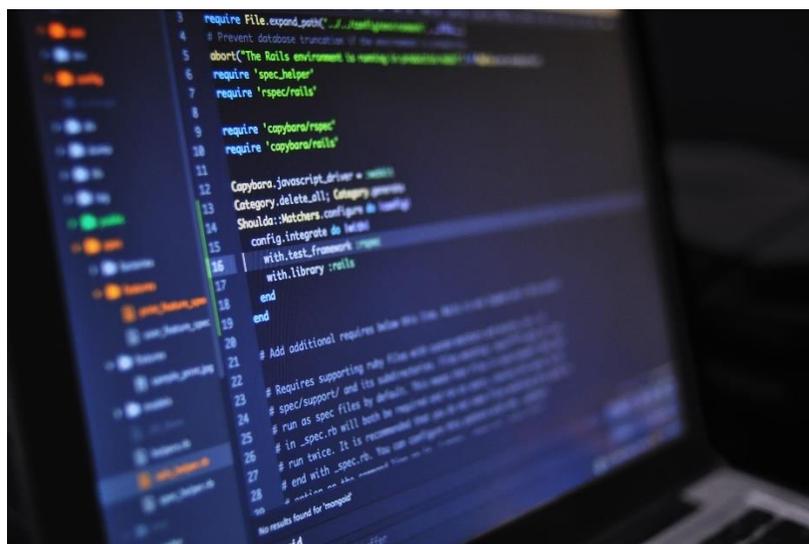
Does the firm require that any client transactions initiated over email be verified with additional information? Does the firm call its clients to verify their request when withdrawal instructions are received via email?

5. Email communications are secured. (If the response is no, proceed to the next question.)

Does the firm use a secure email service? Does the firm store its electronic communications in a secure location (On-site server, cloud-service, etc.)?

6. Employees and clients are aware that email communication is not secured.

If the firm does not use a secure email service, and does not store its communication in a secure location, are clients and employees aware of that information so that they can adjust their business practices accordingly?



## Protect – Devices

1. Device access (physical and digital) is permitted for authorized users, including personnel and clients.

What procedures does the firm have in place to ensure only authorized users are accessing the firm's electronic assets? Does the firm require encryption on all portable electronic devices? Does the firm require a passcode on all firm cell phones?

2. Device access is routinely audited and updated appropriately.

How often does the firm review its practices and procedures to ensure compliance and advancement?

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.)

If the firm was unable to access the information locally stored on certain devices, would the firm still be able to fulfill its business needs?

4. Backups are routinely tested.

A backup of information is not useful if it does not work or contain the correct information.

5. The firm has written policies and procedures regarding destruction of electronic data and physical documents.

How does firm address the disposal of electronic records and devices? Does the firm use the appropriate method to ensure the data is not recoverable? This prevents the firm from unintended and unauthorized disclosure of confidential information.

6. Destruction of electronic data and physical documents are destroyed in accordance with written policies and procedures.

How often does the firm audit its practices to ensure compliance with written procedures? What are the ramifications for a failure to comply with the written procedures? How is discipline handled in such instances?



## Protect – Use of Cloud Services

1. Due diligence has been conducted on the cloud service provider prior to signing an agreement or contract.

Does the firm check to ensure that the third-parties it is entrusting its data to are secure? Is the firm monitoring access to the information to ensure the third-party is executing the contract with the defined scope?

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.

The firm will want to verify that the third-party is equipped to handle any cybersecurity incidents that may occur during the course of business. Does the firm ensure the third-party has a data breach response plan? Do they test the plan to address any issues it may have prior to a cybersecurity event occurring?

3. The firm has a business relationship with the cloud service provider and has the contact information for that entity.

Does the firm execute a specific contract with the third-party that outlines the scope of the relationship, the use and security of data, the length of the relationship, and the expectations of confidentiality?

4. The firm is aware of the assignability terms of the contract.

The firm understands what portions, if any, will be assigned to other parties. Assignability is similar to subcontracting, and the firm will want to be aware of what portions of the contract will be fulfilled by another party.



5. The firm understands how the firm's data is segregated from other entities' data within the cloud service.

Is the firm's data intermingled with the data of other entities also using the same provider? Is the firm's data stored independently of other entities?

6. The firm is familiar with the restoration procedures in the event of a breach or loss of data stored through the cloud service.

Does the firm understand what steps of the disaster recovery process it is responsible for? Has the firm practiced these procedures to ensure they can be effectively and efficiently performed during a disaster situation?

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.

How will the firm address any issues with the third-party it has contracted should its data be unavailable for business use?

8. The firm solely relies on free cloud storage.

If the firm does not have a third-party on contract and only uses free services, is the firm aware of who owns the data that it stores with the free service?

9. The firm has a back-up of all records off-site.

Is the firm prepared to continue business functions in the event that all of its on-site data and devices are destroyed?

10. Data containing sensitive or personally identifiable information is stored through a cloud service.

If the firm stores the non-public information of its clients in a cloud, what safeguards are in place to ensure that confidential information remains that way.

11. Data containing sensitive or personally identifiable information, which is stored through a cloud service, is encrypted.

By encrypting confidential information stored in the cloud, the firm is adding an additional safeguard to protect the non-public information of its clients.

12. The firm has written policies and procedures related to the use of mobile devices by staff who access data in the cloud.

How does the firm address employees access to non-public information while off-site? Are employees required to have security features enabled on those devices? How is that information checked?

13. The cloud service provider (or its staff) has unfettered access to the firm's data stored in the cloud.

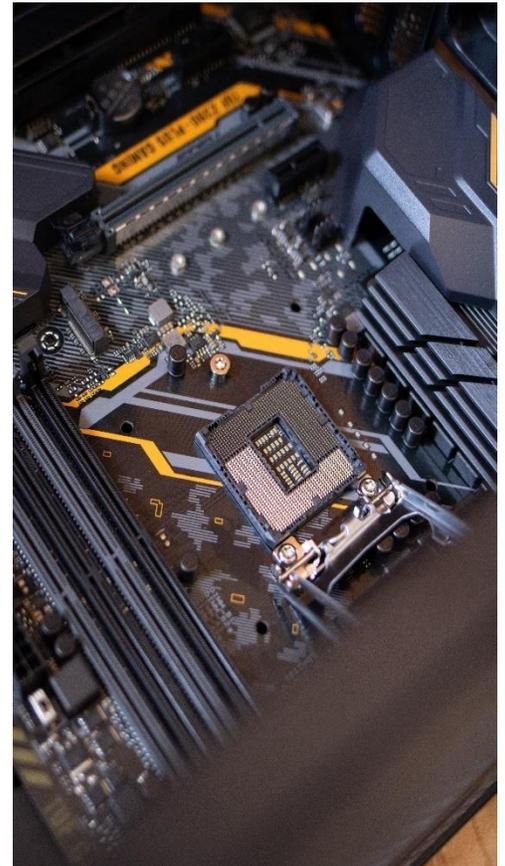
As previously mentioned, is the firm aware of the level of privacy they are obtaining with their third-party service provider?

14. The firm allows remote access to its network (e.g. through use of VPN).

As previously mentioned, are employees authorized to work off-site? If so, what precautions and features are required to increase the security of the firm's information?

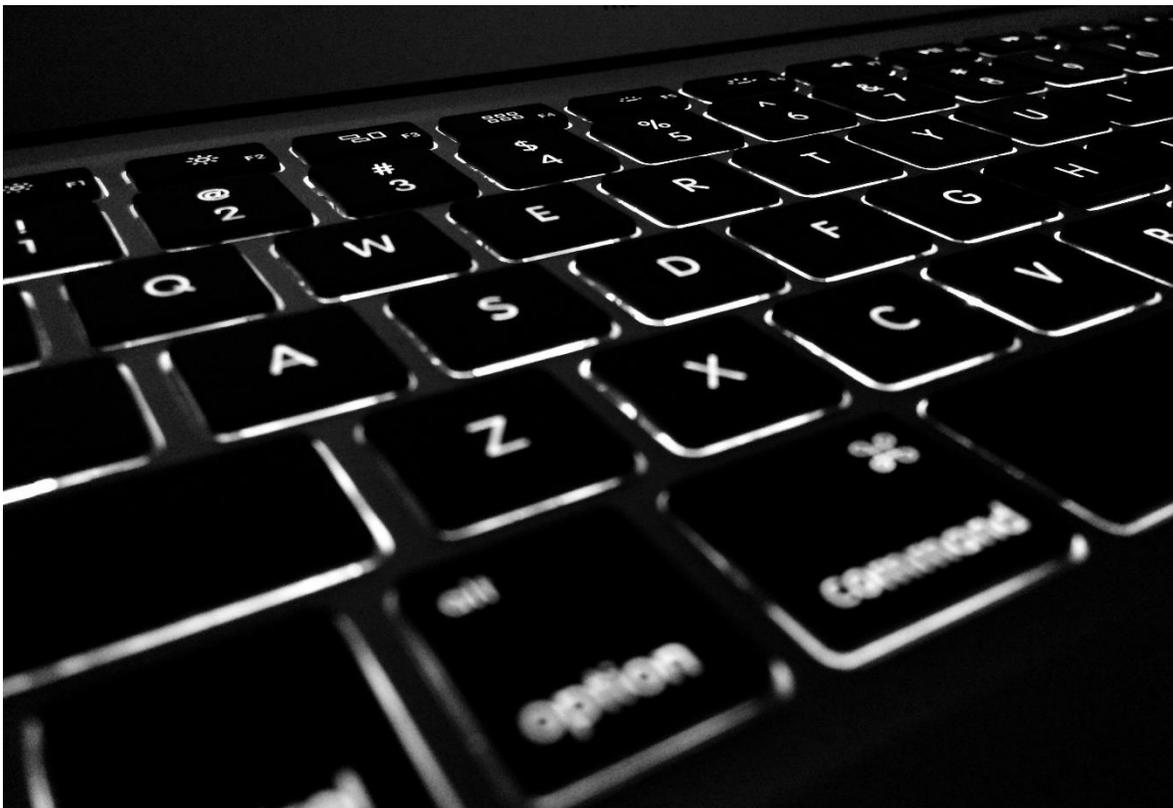
15. The VPN access of employees is monitored.

Does the firm ensure that, even though their traffic is encrypted, employees are using business resources for business purposes and not unnecessarily increasing the firm's likelihood of a cybersecurity breach by visiting unauthorized sites?



16. The firm has written policies and procedures related to the termination of VPN access when an employee resigns or is terminated.

Is employee access “cut-off” prior to their formal termination? If not, how soon after official separation is employee access terminated?



## Protect – Use of Firm Websites

1. The firm relies on a parent or affiliated company for the construction and maintenance of the website.

Who is responsible for updating and managing the firm's website? Is it an affiliate or parent company?

2. The firm relies on internal personnel for the construction and maintenance of the website.



Is there a specific person within the firm that is designated as the firm's webmaster? If so, what is the scope of their responsibility and liability?

3. The firm relies on a third-party vendor for the construction and maintenance of the website.

Who is responsible for updating and managing the firm's website? Is it an external entity?

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.

What due-diligence did the firm conduct prior to executing an agreement with them? Is the firm aware of the scope of privacy granted by their agreement with the third-party? Who is responsible for website data breaches?

5. The firm can directly make changes to the website.

If the firm executed an agreement with a third-party for web services, did the firm maintain control of day-to-day operations?

6. The firm can directly access the domain renewal information and the security certificate information.

Is the firm able to review logs associated with its webpage(s) to ensure the security and accuracy of its public-facing information?

7. The firm's website is used to access client information.

If clients can remotely access their information, what additional steps and safeguards are in place to protect against unauthorized access and disclosure?

8. SSL or other encryption is used when accessing client information on the firm's website.

Does the firm use encrypted sites to add an additional level of security? Is the firm's website accessed through HTTP or HTTPS?

9. The firm's website includes a client portal.

Is there a portion of the firm's website that houses non-public client information that clients must log-in to access?

10. SSL or other encryption is used when accessing a client portal.

As previously mentioned, is this portion of the website accessed through a more secure connection than the other public-facing portions of the website?

11. When accessing the client portal, user authentication credentials (i.e., user name and password) are encrypted.

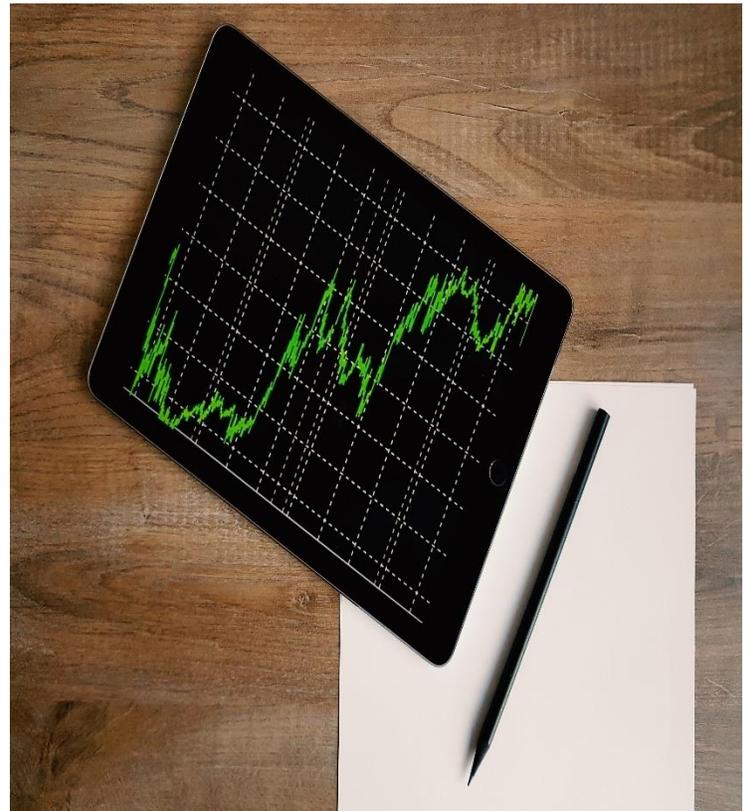
When a client enters their information, is that data encrypted while being transmitted to the firm's webserver?

12. Additional authentication credentials (i.e., challenge questions, etc.) are required when accessing the client portal from an unfamiliar network or computer.

If the client remote access is an anomaly, what additional steps are required to authenticate the client's identity?

13. The firm has written policies and procedures related to a denial of service issue.

If the firm's webpage is inaccessible for any reason, specifically – a DoS attack, how will the firm handle the client impact?

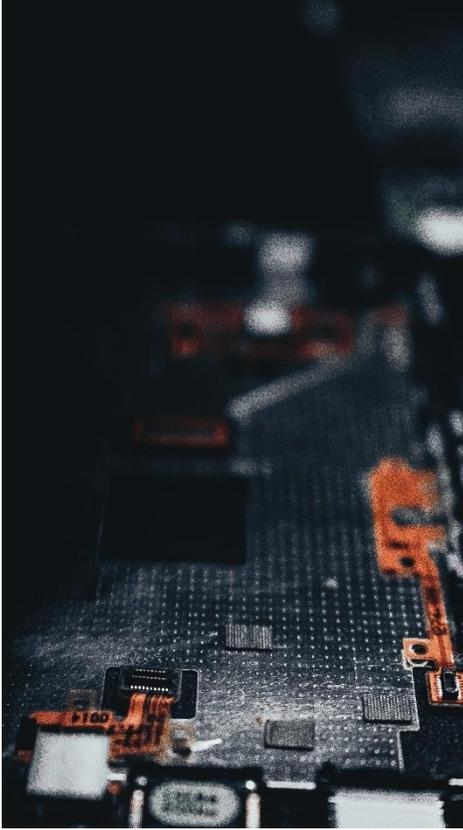


## Protect – Custodians & Other Third-Party Vendors

1. The firm's due diligence on third parties includes cybersecurity as a component.

When executing agreements with external entities, the firm verifies the reputation of the third-party and ensures safeguards are in place to protect any information the third-party will access or possess.

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.



The firm requires any third-parties, with whom an agreement is, or to be, executed, to explain and justify their cybersecurity practices and reviews any written cybersecurity procedures.

3. The firm understands that the vendor has IT staff or outsources some of its functions.

What are the third-parties cybersecurity capabilities? Is it well enough equipped to protect the firm's information?

4. The firm has obtained a written attestation from the vendor that it uses software to ensure customer data is protected.

Has the firm obtained written notice that the third-party actively monitors its electronic assets to verify that unauthorized access or disclosure has not occurred?

5. The firm has inquired whether a vendor performs a cybersecurity risk assessment or audit on a regular basis.

Does the third-party regularly review its cybersecurity practices, procedures, and vulnerabilities to ensure that its systems are secure and that it is protecting the information that it is entrusted with?

6. The cyber-security terms of the agreement with an outside vendor are not voided because of the actions of an employee of the firm.

If the firm has executed an agreement with a third-party, under what circumstances will the contract be terminated? If it is terminated because of the actions of the firm, or one of its employees, what are the ramifications?

7. Confidentiality agreements are signed by the firm and third-party vendors.

Does the firm execute agreements with the third-party that ensure its information, or any information related to a breach, will not be disclosed except as required by law?

8. The firm has been provided enough information to assess the cybersecurity practices of any third-party vendors.

Is the firm aware of the cybersecurity practices of each of the third-parties with which it has executed an agreement? Is the firm comfortable with the practices of those third-parties as they relate to the practices of the specific industry of the third-party?

9. [Relevant to custodians only] The firm has discussed with the custodian matters regarding impersonation of clients and authentication of client orders.

Does the firm discuss with its clients why specific procedures are in place and provide the client with “best practices” to prevent unauthorized access, trades, and withdrawals in their accounts?



## Protect – Encryption

1. The firm routinely consults with an IT professional knowledgeable in cybersecurity.

Is the firm capable of effectively and efficiently securing its electronic resources without the help of a qualified professional? If not, does the firm employ, or contract, a professional to assist with their cybersecurity efforts?

2. The firm has written policies and procedures in place to categorize data as either confidential or non-confidential.

How does the firm classify data stored on its electronic assets? Can the firm account for all confidential information stored within its infrastructure and verify that unauthorized access and disclosure has not occurred?

3. The firm has written policies and procedures in place to address data security and/or encryption requirements.

Within the firm's compliance manual, does the firm have a section addressing the security of its electronic assets and data?

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.).

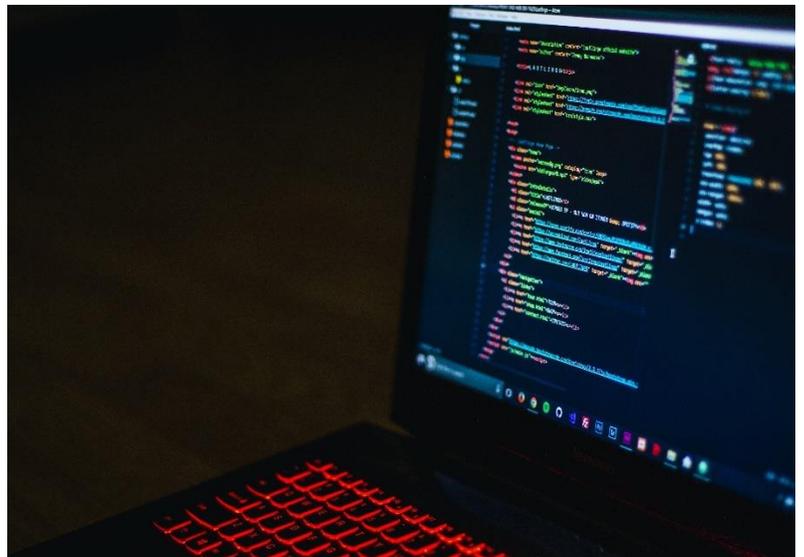
Within the firm's compliance manual, does the firm have a section addressing physical access controls it will utilize to ensure the security of its electronic assets and data?

5. The firm utilizes encryption on all data systems that contain (or access) confidential information.

What safeguards does the firm have in place to ensure that the non-public information it accesses, or stores, is protected from unauthorized disclosure?

6. The identities and credentials for authorized users are monitored.

Does the firm actively scan its electronic assets and infrastructure to ensure that unauthorized access is not occurring?



## Detect – Anti-Virus Protection and Firewalls

1. The firm regularly uses anti-virus software on all devices accessing the firm’s network, including mobile phones.

Does the firm require that an anti-virus program be running on all devices that it authorizes to access its network? If not, does the firm have any requirements for devices that it authorizes to access its network?

2. The firm understands how the anti-virus software deploys and how to handle alerts.

Does the firm have a basic understanding of the purposes and functions of anti-virus software? Arguably more importantly, does the firm understand what anti-virus software does not do?

3. Anti-virus updates are run on a regular and continuous basis.

Does the firm ensure that the “library” of its anti-virus software is consistently and constantly updated? This will ensure that the anti-virus software is current and addresses recently identified virus heuristics.

4. All software is scheduled to update.

Are software patches set to manually update or will the system update software automatically? Automatic updates remove the time-commitment of manually ensuring that software is updated as patches become available.



5. Employees are trained and educated on the basic function of anti-virus programs and how to report potential malicious events.

Are the firm’s employees aware of their roles and responsibilities when they suspect the firm has suffered a cybersecurity event?

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.

Is there an executed agreement between the firm and any third-party services providers from which it is obtaining services?

7. A firewall is employed and configured to appropriate to the firm’s needs.

Does the firm understand the basic functions and importance of utilizing a firewall? Does the firm understand the functions and settings of its firewall and ensure that it is satisfying the firm’s needs?

8. The firm has policies and procedures to address flagged network events.

Does the firm have written policies and procedures outlining how the it will mitigate the occurrence of a suspected cybersecurity event?

## **Respond – Responding to a Cyber Event**

1. The firm has a plan and procedure for immediately notifying authorities in the case of a disaster or security incident.

Does the firm understand its legal obligations in the event of a cybersecurity event?

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.

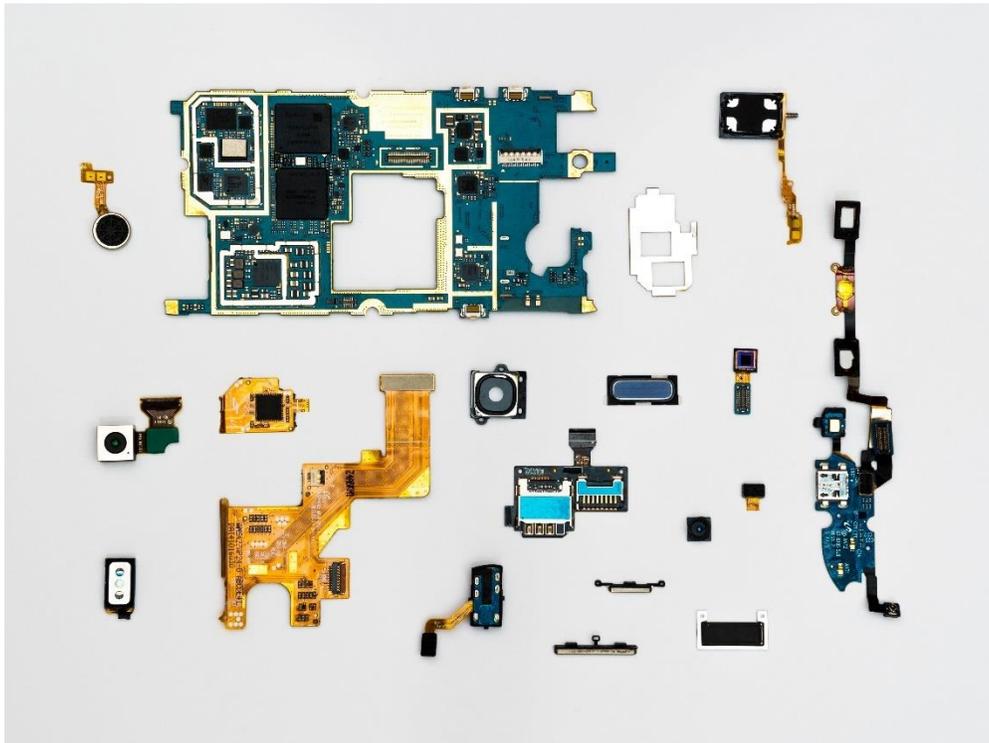
Do the firm's written policies and procedures document the authoritative bodies to which it must report the occurrence of specific events?

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.

Do the firm's written policies and procedures document the internal parties responsible for handling external communication? Do the policies and procedures outline the ramifications for unauthorized parties communicating the occurrence of a cybersecurity event to external parties?

4. The communications plan identifies the process for notifying clients.

Do the firm's written policies and procedures address the internal parties responsible for communicating a cybersecurity event to the firm's clients? Do the policies and procedures document how promptly the event's occurrence will be communicated to clients?



## Recover – Cyber-insurance

1. The firm has considered whether cyber-insurance is necessary or appropriate.

Is the firm legally, or contractually, required to maintain cyber-insurance? If not, does the firm feel that cyber-insurance is appropriate considering their business model and the associated risks?

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).

Is the firm aware of the limits of its coverage? Does the firm understand specifically what events are, and are not, covered?

3. The cybersecurity insurance policy covers notification (clients and regulators) costs.

Is the firm aware of the extent of coverage and total expenses allotted to cover costs by the cyber-insurance it obtained?

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).

Does the firm understand the specific events whose occurrence are not covered by its cyber-insurance? How does the firm plan to mitigate those events?

5. The exclusions of the cybersecurity insurance policy are appropriate for the firm's business model.

Has the firm evaluated its business practices/needs and determined the cybersecurity events excluded by its cyber-insurance policy are not events that it desires to be covered?

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.

Does the firm understand the specific actions and steps it is required to take to ensure the cyber-insurance policy remains in effect? How does the firm mitigate the occurrence of events that would void its policy?

```
<div class="container">
  <div class="row">
    <div class="col-md-6 col-lg-8"> <!-- BEGIN NAVIGATION
      <nav id="nav" role="navigation">
        <ul>
          <li><a href="index.html">Home</a></li>
          <li><a href="home-events.html">Home Events</a></li>
          <li><a href="multi-col-menu.html">Multiple Column Men
          <li class="has-children"> <a href="#" class="current"
            <ul>
              <li><a href="tall-button-header.html">Tall But
              <li><a href="image-logo.html">Image Logo</a></li>
              <li class="active"><a href="tall-logo.html">Ta
            </ul>
          </li>
          <li class="has-children"> <a href="#">Carousels</a>
            <ul>
              <li><a href="variable-width-slider.html">Variab
              <li><a href="variable-width-slider.html">Testimoni
```

## Recover – Disaster Recovery

1. The firm has a business continuity plan to implement in the event of a cybersecurity event.

Does the firm have a written plan addressing how it will respond to the occurrence of a cybersecurity incident? Has the firm tested this plan to ensure that it properly works prior to the occurrence of a cybersecurity incident?

2. The firm has a process for retrieving backed up data and archival copies of information.

Does the firm maintain data back-ups? Is the firm aware if these back-ups are stored on-site or off-site? Has the firm tested the back-ups to ensure they function and contain the intended information?

3. The firm has written policies and procedures for employees regarding the storage and archival of information.

Does the firm document, in writing, the roles and responsibilities of its employees should the disaster recovery process be required? Is it stored in a location that employees are still able to access the information in the event of a cybersecurity incident?

4. The firm provides training on the recovery process.

Are employees trained on the written policies and procedures and their responsibilities during the recovery process? Is this training documented to ensure the firm complies with its written policies and procedures? Are ramifications for non-compliance explicitly documented?

