2018

The Maine Office of Securities Cybersecurity Guidelines

Recommendations from the Maine Cyber Security Cluster

John Couch

Katrina Sabochick

Maine Cyber Security Cluster

Abstract

The Maine Office of Securities and the Maine Cyber Security Cluster have partnered together to develop materials intended to assist Maine licensed investment advisers in securing sensitive client information and data in their possession. It has become apparent that the firms could benefit from increased education regarding cybersecurity threats and protections. This guide was developed to fill this gap in information, ensuring that sensitive personal and financial information obtained by investment advisors is protected from known cybersecurity risks.

The information provided in this guide is for your convenience only and is not intended as legal advice. Always seek assistance from legal and technical professionals.

Table of Contents

Introduction

Cybersecurity-related attacks on sensitive data have become more and more prevalent in information security. New types of incidents are identified constantly. Prevention tools and policies are crucial for avoiding attacks, but as not all events can be avoided, it is important to have definitive guidelines to follow for incident response.

The purpose of this guide is to assist Maine investment advisers in securing sensitive client data against potential cyber-attacks. The guidelines are based on the Cybersecurity Checklist for Investment Advisers published by the North American Securities Administrators Association (NASAA).[1]

The guide is divided into five sections - Identify, Protect, Detect, Respond, and Recover. Each section is designed to address the specific recommendations for cybersecurity. However, it is important to note that the needs for each firm will vary widely depending on the size and scope of the firm. These guidelines are designed to be broad enough to apply to most investment advisers licensed in Maine.

At the end of this guide there are three appendices to assist with interpretation. Appendix A contains common terms and definitions used throughout the guide. Appendix B contains a checklist that can be used by investment advisers when entering business relationships with third party vendors to ensure that cybersecurity requirements are met. Appendix C contains specific legal resources, provided by the Maine Office of Securities, that apply to data protection for investment advisers.

[1] For more information on cybersecurity from NASAA, please visit www.nasaa.org.

Guide Overview

Function	Category	Summary
Identify	Risk Assessment	Documenting how the firm currently handles risk internally and externally
Protect	Electronic Mail	Documenting current and future use of email, from transmission to account authentication
	Devices	Identifying authorized users on firm devices and backups of device information
	Cloud Services	Understanding the nature of cloud services and how the third party vendor is handling information
	Firm Websites	Knowing who manages and makes changes to a firm's website and how users connect to it
	Third-Party Vendors	Establishing a contract with a third-party that outlines cybersecurity practices
	Encryption	Securing sensitive communications and data with encryption
Detect	Anti-Virus Protection and Firewalls	Putting passive systems in place to monitor and protect a system from malicious actors
Respond	Responding to a Cyber Event	Outlining a policy to follow in the event of a cyber attack
Recover	Cyber-insurance	Compensating for a potential cyber incident through risk transfer
	Disaster Recovery	Writing and testing a business continuity plan and disaster recovery

Identify: Risk Assessments & Management

The purpose of identification is to evaluate potential risks and hazards regarding all aspects of cybersecurity. The steps below should be treated as a checklist - each aspect of risk assessment should be covered thoroughly and with adequate documentation.[2]

1. Risk assessments are conducted frequently (e.g. annually, quarterly).
A risk assessment is a way to "identify potential hazards and analyze what could happen if a hazard occurs."[3] The goal is to take what has been identified as an asset and plan out what to do in the event an incident occurs. Because potential hazards can change frequently, it is the responsibility of the firm to perform risk assessments on a regular basis.

2. The risk assessment includes a review of data collected/created, where the data is stored, and if the data is encrypted.
For all data stored by the firm, including employee and client information, a comprehensive review of how and where the data is stored is required. This includes listing any third party services used to store the data (i.e., cloud services) as well as how the data is encrypted.

3. Internal "insider" risk and external risks are included in the assessment.
All types of risks should be evaluated, including "insider" risks. These consist of risks from disgruntled employees that may abuse access to sensitive data, as well as employees with inadequate training or incorrect levels of access.

4. The risk assessment includes relationships with third parties.
Include any third party vendor in the risk assessment. This includes cloud service and storage, software maintained by a third party, and physical services such as building security.

5. Adequate policies and procedures demonstrate expectations of employees regarding cybersecurity practices.
Procedures that protect against potential hazards should be listed in a clear and concise manner for employees. Examples include frequent password changes, locking devices, and policies for reporting lost or stolen devices.

---

[2] The information provided here is based on guidelines published by the North American Securities Administrators Association (NASAA). For more information, visit www.nasaa.org.

[3] "Risk Assessment." *Risk Assessment | Ready.Gov*, Department of Homeland Security, 2017, www.ready.gov/risk-assessment.

6. Primary and secondary person(s) are assigned as the central point of contact in the event of an incident with specific roles and responsibilities.

In the event of a breach, a central point of contact (the "primary") is the person(s) who should be notified immediately. This person(s) will be responsible for implementing the plan of action. Secondary person(s), often IT staff or management, should also be identified and assigned as points of contact in the event of an incident.

Depending on the data affected, it may be beneficial to assign different secondary person(s) for different types of attacks. In addition to technical secondaries, a tertiary point of contact to handle media communications may be necessary in the event of a breach.

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

An inventory of all hardware and software is crucial to detecting attacks. To be useful, the inventory should be updated and maintained regularly to ensure that all devices are accounted for.

Protect: Use of Electronic Mail

Email is the most common method of communication used in business discussions. It is important to understand email security to assess what kinds of data are appropriate for the given level of security. This list should be reviewed periodically to assess the security of email communications between employees and clients.

1. Identifiable information of a client is transmitted via email.
Though this may seem like a rudimentary step, it is important for both the employees and the clients to understand what kind of information is appropriate to send via email. The firm should have established guidelines for the types of data permitted through email.

2. Authentication practices for access to email on all devices (computer and mobile) is required.
Proper authentication procedures for email access help prevent unauthorized access to sensitive information. Generally, two-factor authentication should be standard in accessing email, particularly on mobile devices.

3. Passwords for access to email are changed frequently.
Frequent password changes help prevent unauthorized access. In addition, password changes prevent terminated employees from continuing to have access to sensitive data.

4. Policies and procedures detail how to authenticate client instructions received via email.
When receiving instructions from a client regarding personal or financial information, it may be necessary to establish multiple methods of authentication. This ensures that the instruction is valid and not the result of a breach or unauthorized access.

5. Email communications are secured. If not, employees and clients are both aware that they are not secured.
Email communications, particularly between the employees and the clients themselves, should be secure. Modern email applications, also known as clients, such as GMail® and Microsoft Outlook® provide secure communications through encryption, and some email clients provide additional security, but no method of communication is perfect.[4]
Both employees and clients should be aware of the level of security of email communications. If one party is not comfortable with that security, a different method of communication or additional authentication may be used.

[4] Email clients that provide more secure levels of encryption typically require a monthly fee, which may not be appropriate for the client.

Protect: Devices

Devices used by investment firms cover a wide range of functions. Filing systems, mobile electronic devices, and data servers are just a few examples of commonly used tools. Policies and procedures outlined by the firm should be specific for each type of device, from updating and maintaining backups to access levels to the destruction of the stored data. The list below is a general overview of areas that should be outlined in written policies and procedures.

1. Device access (both physical and digital) is permitted for authorized users, including personnel and clients.
Access to devices - which can include computers, cell phones, tablets, and servers - is part of everyday work. However, different levels of access may be appropriate, particularly for any device that can access stored data or sensitive information. A good rule of thumb is to follow the "principle of least privilege," where each person is given only the minimum level of access to complete their work. This adds an additional layer of security regarding "internal" risks.

2. Device access is routinely audited and updated appropriately.
It is important to consistently review and update levels of device access. As employees and clients are let go or added, outdated levels of authorization can pose a potential internal security risk. The general recommendation is to establish policies for access levels upon taking on a client or employee and upon termination, as well as routinely auditing device access and updating them appropriately.

3. Devices are routinely backed up, underlying data is stored separately, and backups are routinely tested.
Backups for devices (both physical and digital) are extremely important to maintain in the event that a device is lost, stolen, or otherwise compromised. The underlying data for the device - login information, recovery processes, and backup procedures - should be stored separately as to ensure that backups can be utilized in the event of a compromised device. The backups should also be routinely tested and updated.

4. The investment adviser has written policies and procedures regarding destruction of electronic data and physical documents, and these policies and procedures are followed accordingly.
The destruction of electronic data and physical documents is crucial in preventing breaches, particularly with sensitive or personal data. The destruction of electronic data should follow

standard practices[5], which can differ from device to device. For physical documents, standard practices typically include using cross-cut shredders, incinerators, or other methods to permanently destroy documents. When devices are discarded, it is important to ensure that no data remains (e.g., laptop hard drives). The policies and procedures regarding the destruction of data should be clearly outlined and updated as new technologies are added to the firm's use.

[5] For specific information regarding the destruction of electronic data, visit the National Institute of Standards and Technology website at www.nist.gov

Protect: Cloud Services

In general terms, cloud services refers to any storage and access of data and programs over the Internet, instead of on a local hard drive or filing system. Cloud service providers are third-party vendors that help manage this data over a network. As the use of cloud services is relatively new, some policies and procedures may be unfamiliar to firms. This section aims to break down the guidelines that should be followed when utilizing cloud computing to store and manage personally identifiable information (PII).

1. Due diligence has been conducted on the cloud service provider prior to signing an agreement or contract.
The agreement or contract between the investment adviser and the cloud service provider should be clear and specific in satisfying the legal requirements for the protection of stored data. This contract should include options for updating or amending these requirements as new technology is released and/or new standards set in place by government services.

2. The investment adviser has evaluated whether the cloud service provider has safeguards against breaches as well as a documented process in the event of breaches.
As cloud services typically store large amounts of sensitive data, it is crucial for the investment adviser to evaluate whether the cloud service provider has reasonable and up-to-date safeguards against breaches. The cloud service provider should also have a documented process in the event of breaches, which adheres to legal requirements and is satisfactory for both parties.

3. The investment adviser has a business relationship with the cloud service provider, has up-to-date contact information, and is aware of the assignability terms of the contract.
As standard practice, the business relationship between the investment adviser and the cloud service provider should be updated when appropriate, including with contact information and terms of the contract. Assignability terms should also be fully outlined and understood in the event of a transfer of services or delegation of responsibilities.

4. The investment adviser understands how the firm's data is segregated from other entities' data within the cloud service.
As cloud service providers typically store data for multiple clients, it is important for the adviser to understand how separate the firm's data is from others. In the event of a breach on another entities' data, this separation could mean the difference between a breach on the firm and a simple security warning.

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

In the event of a breach, it is important for the investment adviser to know the cloud service provider's procedures to restore data. These procedures may include the incorporation of backups, policies regarding client notification, and other guidelines to ensure maximum data recovery. The restoration procedures should be outlined and approved by the investment adviser prior to signing the agreement or contract.

6. The investment adviser has written policies and procedures in the event that the cloud service provider is purchased, closed, or otherwise unable to be accessed.

Just as the adviser should be aware of the assignability terms of the contract, the investment adviser should have written and agreed upon policies and procedures should the cloud service provider be altered in any way.

7. The investment adviser has a backup of all records off-site.

Generally, it is recommended that firms follow the "3-2-1" rule for backing up data - three total backups, two that are local but on different mediums, and one offsite.[6] This offsite backup ensures that in the event that the firm's physical location is compromised in any way, important data is kept secure and able to be restored.

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

Encryption should be used for all sensitive data.[7] Most cloud services come with encryption as a standard application, but it is important for the investment adviser to know the specifics of the encryption used and whether it is appropriate for the data.

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

When the investment adviser is constructing policies and procedures for the use of devices by their staff, those employees who have access to data in the cloud have specific instructions regarding the use of their mobile devices.

---

[6] For more information on how to implement the 3-2-1 backup guideline, visit https://www.backblaze.com/blog/the-3-2-1-backup-strategy/

[7] For more specific information regarding encryption, see Protect: Encryption in this guide.

10. The cloud service provider's access to the investment adviser's data stored in the cloud is understood by both parties.

As the cloud service provider will be storing and handling sensitive information, the agreement between the firm and the provider should include the amount of access and confidentiality that the provider must adhere to.

11. The investment adviser has written policies and procedures regarding remote access to the stored data (e.g. through use of VPN).

Just as with mobile devices, those employees who can access the stored data remotely (for both cloud service provider employees and the firm's staff) should have specific instructions regarding their use of remote access. This may include requirements for the levels of encryption and protection that the VPN utilizes. It is best that the technical information regarding remote access policies be established by the firm's IT department.[8]

[8] In this guide, when "the firm's IT department" is mentioned, it is understood that this includes any third-party vendors that handle IT services for the firm.

Protect: Websites

As almost all firms have websites for clients to access, it is important to establish proper security and protection of the website. It is up to the investment adviser to decide how comprehensive the services provided by the website will be (e.g., a client portal) and how much access employees will be given. Regardless of the level of complexity, proper security protocols should be adhered to in order to protect client and company information in the event of a breach.

1. The team and/or vendor that is responsible for the construction and maintenance of the website is in agreement with the investment adviser regarding services and confidentiality.
The firm may use a parent company, internal personnel, or a third-party vendor to construct and maintain the website. Regardless of the responsible party, the investment adviser should maintain an agreement with the party regarding services and confidentiality.

2. If desired, the investment adviser can directly make changes to the website.
If the investment adviser wishes to be able to make changes to the website directly, they should have an agreement with the responsible party regarding the method of access (i.e., remote through VPN, login information, etc.). Additionally, there should be written policies and procedures for notification if the responsible party makes technical adjustments to the site that affect the investment adviser's access.

3. The investment adviser can directly access the domain renewal information and the security certificate information.
In order to ensure that proper security protocols are followed, the investment adviser should have direct access to the updated domain renewal and security certificate information. This documentation should be updated and maintained regularly.

4. If the firm's website is used to access client information, TLS or other encryption is used when accessing client information on the firm's website.
If client information can be accessed through the website - whether by data storage or through a client portal - encryption should be used when accessing the data. The recommended method of encryption will vary according to your needs and should be mandated by the firm's IT department in conjunction with the responsible party.[9]

[9] For more information on encryption, see Protect: Encryption in this guide.

5. If the firm's website includes a client portal, TLS or other encryption is used when accessing a client portal.

If clients can access and/or store their own data through a client portal included in the website, encryption should be used. The recommended method of encryption will vary according to your needs and should be mandated by the firm's IT department in conjunction with the responsible party.

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

In addition to ensuring proper levels of encryption, other security measures should be implemented when the access attempt comes from an unfamiliar network or computer. This may include additional verification such as using two-factor authentication or requiring a temporary PIN.

7. The investment adviser has written policies and procedures related to a denial of service issue.

Denial of service consists of the disruption of services of a host connected to the Internet (e.g., a website). This is one of the most common malicious attacks on a website, and is typically accomplished by flooding the targeted site with requests and overloading the system. Because this type of attack is so common, the investment adviser and the responsible party should have agreed upon policies and procedures regarding the response to such an event. The responsible party should demonstrate that they have the proper resources to handle an attack, to the satisfaction of the firm.

Protect: Third Party

Third party vendors are a necessary part of any business. Custodial staff, catering services, cloud storage, and printing services are just a few vendors that may have agreements with the firm. For each third party used, it is vital to ensure that their cybersecurity practices adhere to industry standards. These standards will differ for each vendor, but the general guidelines presented here can be applied to all third parties used by the investment adviser.

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

Any third party, regardless of their involvement in data storage or technology, must have a clearly stated and mutually understood agreement regarding cybersecurity. This component will look different for each party, but general requirements should be outlined and agreed upon prior to entering the arrangement. This may include third party staff's mobile devices, connections to WiFi or websites, or confidentiality agreements regarding technology onsite.[10]

2. The investment adviser has requested vendors to complete a cybersecurity questionnaire, with a focus on the issues of liability sharing and whether vendors have policies and procedures based on industry standards.

Using a questionnaire to evaluate whether the vendor has adequate policies regarding cybersecurity can streamline the due diligence process. This questionnaire should adhere to industry standards and those particular to the specific technologies used by the firm. An overview of what topics should be addressed can be found in Appendix B of this guide.

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

Many third party vendors will have their own IT staff and cybersecurity standards. Upon entering an agreement, the investment adviser should be aware of IT staff or outsourced parties that may handle or oversee parts of the relationship between the vendor and the investment adviser.

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

Any customer data handled or stored by a third party must be proven to be protected. In addition, this protection software must be regularly updated and maintained. The investment adviser should obtain a written confirmation of this protection that is updated when necessary.

---

[10] For more information on the legal obligations concerning confidentiality, see Appendix C: Legal Resources of this guide.

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

Risk assessments, which may involve penetration testing, are used to evaluate strengths and weaknesses in cybersecurity. The exact nature of these risk assessments may vary depending on the nature of the third party. Regardless of the structure, the investment adviser should be fully informed on these procedures upon entering an agreement with the vendor.

6. The cybersecurity terms of the agreement with an outside vendor is <u>not</u> voided because of the actions of an employee of the investment adviser.

As with any agreement, policies and procedures regarding the responsibilities of each party should be clearly stated and mutually understood. It is recommended that no actions of an employee of the investment adviser should result in the cybersecurity agreement being voided, as the vulnerability of client data and PII is of higher priority than the actions of an employee. Specific cases may warrant further discussion with the vendor regarding this policy.

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

Again, as with any agreement, confidentiality policies and procedures should be clearly stated and mutually understood. These agreements should adhere to industry standards (see Appendix C of this guide for the legal requirements specific to investment advisers and PII).

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

With the questionnaire, confidentiality agreements, and risk assessments, the investment adviser should have a thorough understanding of the cybersecurity practices for all vendors. If the investment adviser does not feel that they have covered all necessary areas, additional information should be requested before entering an agreement. It may also be necessary to allow the IT staff of the firm to evaluate the cybersecurity practices independently to ensure that policies for each kind of software used are followed to industry standards.

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

Data custodians oversee the custody and storage of data at the firm as a part of the IT staff. This includes authorization procedures for both clients and staff, and managing orders from clients regarding access to their data. The investment adviser must ensure that the data custodian follows proper policies and procedures regarding authentication. Risk assessments and penetration testing can ensure that the custodian is following these procedures.

Protect: Encryption

The protection of confidential data consists of many methods, and the most commonly used is encryption. Encryption is the process of encoding information so that only authorized users can access it. Though some encryption schemes can be cracked, this is the best tool for protecting confidential information from malicious actors.

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

Due to the constantly changing nature of cybersecurity, it is important for the investment adviser to regularly consult with IT professionals about protection and security. It is recommended to use an external consultant to evaluate the strengths and weaknesses of the current procedures of the firm, typically in the form of a risk assessment that may involve penetration testing. These consultations should take place on a regular basis (quarterly or semi-annually, depending on the size and scope of the firm) as well as whenever large scale changes are made (firm-wide software updates, new physical location, etc.).

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

The classification of data is used to determine the level of encryption that should be used to protect it. The general requirement for confidential information is defined as "any client information that an investment adviser must keep private."[11] This may be broken up into levels of confidentiality depending on the amount of data and the needs of the firm, but every piece of data should be assigned a confidentiality designation.

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

Once the data has been assigned a confidentiality level, written policies and procedures should dictate the exact level of security and encryption required. This security must be maintained and regularly updated to protect against new types of breaches. Encryption should adhere to industry standards for the software and/or technology being used (e.g., TLS encryption protocols[12]) as dictated by IT staff.

---

[11] For more information on the definitions regarding confidential information, see Appendix C: Legal Resources of this guide.

[12] TLS is defined more thoroughly in the Appendix A: Terms and Definitions of this guide.

4. The investment adviser 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.).

Physical security of devices is often overlooked concerning data security, but is one of the most common methods used by malicious actors in the event of a breach. The investment adviser must ensure that all employees follow proper protocols regarding the physical access to devices containing confidential data.[13]

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

As stated previously, encryption should be used on all confidential data. However, this also includes any device that can access the data remotely (e.g., a cell phone connected to the firm's network), which is often overlooked. The level of encryption on these secondary devices should be established by IT staff when necessary.

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

Encryption may protect data from strangers, but a malicious actor with false credentials may gain access to data regardless. The identifications for authorized users must be updated regularly as employees join or leave the company, and passwords should be changed often. IT staff should also use network traffic monitoring systems (i.e., Wireshark) to identify potential anomalies in traffic and logins.

[13] For more specific information regarding physical devices, see the Protect: Devices section of this guide.

Detect: Anti-Virus Protection and Firewalls

While protection methods may provide safeguards against attacks, it is equally important to know when attacks take place. Anti-virus software, firewalls, and regular log reviews are all good methods of detection that help to prevent malicious activity.

1. The investment adviser firm regularly uses anti-virus software on all devices accessing the firm's network, including mobile phones.
Anti-virus software for all devices - computers, servers, and mobile phones included - should be required and maintained regularly. The software should provide an alert system in the case of a detected attack, as well as specific information about the attack and assistance with protection from and removal of any malicious files.

2. The investment adviser understands how the anti-virus software deploys and how to handle alerts.
It is important to not only have anti-virus software installed, but to thoroughly understand how the software functions. From device to device, the firm may have different types of software to handle virus detection, and each of these types may have different alert systems. The investment adviser must be aware of these different systems and check them accordingly.

3. Anti-virus updates are run on a regular and continuous basis.
As with any software, anti-virus applications should be updated regularly. Since new types of attacks are constantly being discovered, outdated software may not be able to detect all known types. Updates allow the software to recognize each type and respond accordingly.

4. All software is scheduled to update.
All software, from word processors to accounting applications, has safeguards for protecting data. While updating anti-virus software is essential to detecting all forms of attack, *all* software should be updated regularly to protect any data stored in the applications used by the investment adviser.

5. Employees are trained and educated on the basic function of anti-virus programs and how to report potential malicious events.
As a part of regular training, all employees of the firm should understand the basics of anti-virus software. Notifications about potential attacks come in different forms that should be able to be recognized by all members. In addition, the proper protocol for reporting suspected malicious activity should be clear to all employees.

6. If the alerts are set up by an outside vendor, there is an ongoing relationship between the vendor and the investment adviser to ensure continuity updates.

The detection software may be managed by an outside vendor or IT company, particularly if the firm handles many clients. The investment adviser should maintain consistent communication with the vendor.[14]

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

Firewalls are used to monitor and control network traffic. The use of a firewall enables the user to detect any unauthorized activity in the firm's network. The IT department of the firm should fully implement, update, and maintain a firewall or firewalls. The configuration of the firewall(s) will vary depending on the needs of the firm, and may change as the investment adviser takes on additional clients or adjusts the responsibilities of the firm.

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

In the event that malicious activity is detected or flagged by the firewall, there must be a clear and thorough protocol for addressing the event. The investment adviser may choose to address certain types of suspicious activity differently, such as investigating unauthorized network access or implementing new safeguards. In addition, the proper notification process should be understood by all employees to ensure that the event can be dealt with as quickly as possible.

[14] For more information about maintaining relationships with outside vendors, see Protect: Third Party Vendors of this guide.

Respond: Responding to a Cyber Event

In the event of an attack, the investment adviser should have an established response plan. The plan should include instructions for notifying authorities and clients, assembling a response team of employees, and investigating the reason for the breach. Legal requirements may apply to the cyber event.

1. The investment adviser has a plan and procedure for immediately notifying authorities in the case of a disaster or security incident.
In the event that any part of the firm is attacked or the data is breached, the investment adviser should have a clear, structured plan for notifying authorities. If client data is affected, notifying authorities helps to rectify the issue as quickly as possible.[15]

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.
Different types of incidents will require different authorities to contact. This may include state regulators, consumer reporting agencies, and any third-party vendors affected. Depending on the nature of the event, the investment adviser also may have a plan for notifying law enforcement.[16]

3. The investment adviser has a communication plan, which identifies who will speak to the public/press in the case of an incident and how internal communications will be managed.
In the event that client data is affected, announcing the breach and communicating to the press is an essential part of the response process. In order to maintain transparency, the investment adviser should have a plan for dealing with the public. Additionally, an internal communication plan for handling the incident should be established. This may include the designation of a response team to coordinate the necessary steps.

4. The communications plan identifies the process for notifying clients.
In the event that client data is affected, the investment adviser should notify clients in a timely manner in accordance with applicable laws. It is the responsibility of the firm to communicate with clients and inform them of breached data, steps the firm will be taking, and any changes that may happen over the course of the investigation.

---

[15] For specific information regarding the legal requirements in the event of a breach, see Appendix C: Legal Resources of this guide.

[16] The Federal Trade Commission (FTC) provides a business data breach response outline. For more information, visit www.ftc.gov

Recover: Cyber-insurance

In the event of a breach, the firm may have many expenses for investigation, notification of clients and regulators, and response. Cyber-insurance policies can help mitigate costs and enable the investment adviser to respond to the attack. The firm should review all elements of the policy to ensure that the coverage is appropriate before deciding whether to purchase coverage.

1. The investment adviser has considered whether cyber-insurance is necessary or appropriate for the firm.
Cyber-insurance is generally recommended for businesses that handle sensitive or financial data for clients. If financially feasible, the investment adviser should decide whether to purchase cyber-insurance to protect themselves and their clients, particularly if the firm handles many clients.

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. an employee who steals sensitive data); and breaches as a result of third-party relationships.
Cyber-insurance can cover a variety of different cyber events. The firm should review all options and decide whether they apply. It is generally recommended to cover, at a minimum, insider and third-party breaches, as these are the most common types of events. The investment adviser should decide if other types of events, such as foreign intruders, apply to the firm.

3. The cybersecurity insurance policy covers notification (clients and regulators) costs.
No matter what the investment adviser decides in terms of event coverage, notification costs should be covered by the cyber-insurance policy. As notification is required by law, it is essential that the firm have the necessary coverage to notify all parties in the event of a breach.

4. The investment adviser 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).
The investment adviser should fully understand the coverage of the cyber-insurance policy. Both first-party coverage (damages to the firm) and third-party coverage (expenses regarding clients and notification). Generally, both types of coverage should be included in the cyber-insurance policy.

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

When the investment adviser decides on the cyber-insurance policy appropriate for the firm, it must be fully understood that any exclusions of the policy are the responsibility of the adviser. The firm should be clear on what risk it is retaining.

6. The investment adviser has put into place all safeguards necessary to ensure that the cybersecurity policy is not voided through investment adviser employee actions, such as negligent computer security where software patches and updates are not installed in a timely manner.

In the event of a breach, it is important for the investment adviser to be aware of any part of the cyber-insurance policy that may void the coverage. If the firm does not maintain proper computer and network security and update regularly, the cyber-insurance policy may be voided. The investment adviser should understand the exact actions that would void the policy and follow the requirements dictated.

Recover: Disaster Recovery

Once an event has taken place and data is compromised, the firm must have the ability to recover data from archives or backups. A comprehensive and detailed recovery plan that includes data retrieval is essential to business continuity, and the investment adviser should ensure that all data is recoverable both thoroughly and efficiently.

1. The investment adviser has a business continuity plan to implement in the event of a cybersecurity event.
Should a cyber event occur, the investment adviser should have a continuity plan to ensure that the day-to-day responsibilities of the firm continue to operate. While the affected data is investigated, the firm may still have clients to manage and therefore must be able to isolate the compromised data to continue running the business.

2. The investment adviser has a process for retrieving backed up data and archival copies of information.
The investment adviser may need to rely on backed up data to restore compromised information. Depending on the backup methods used, this process may include contacting third-party vendors that handle backed up data. It is therefore essential that the firm maintains and updates backups on a regular basis to ensure that the data can be recovered in the event of a breach.[17]

3. The investment adviser has written policies and procedures for employees regarding the storage and archival of information.
Since backups are so essential to the recovery process, all employees must be aware of the policies and procedures regarding data storage. Sensitive or financial data should have clearly written policies that all employees are trained on and follow.

4. The investment adviser provides training on the recovery process.
Recovering compromised data can be a complex task with many elements, including identifying areas of breach and retrieving archived data. It is recommended that the investment adviser provide comprehensive training to employees on this process. In the event of a breach, the firm must be able to react quickly and efficiently to recover as much data as possible.

[17] For more information on data storage and archives, see Protect: Cloud Services of this guide.

Appendix A: Terms and Definitions

3-2-1 Backup - a backup strategy where data is copied to 3 different storage mediums, 2 of those copies are onsite, and 1 copy is offsite.

Anti-virus Software - Computer software that aids in the detection and removal of malicious software.

Authentication Credentials - A way to prove or verify the identity of a user. This is achieved through one or more of the following ways:

- What the user *knows*: something committed to memory, typically a username and password, or username and PIN.
- What the user *has*: some physical thing, typically an ID card, or token like device.
- What the user *is*: a characteristic of a person, typically some sort of biometric, like a fingerprint, iris scan, or face scan.

Availability - The concept that asserts that information systems can be accessed and used when needed.[1]

Backup - A backup is a copy of data stored on another device.

Business Continuity Plan (BCP) - The practiced policies and procedures put into place to ensure the business can continue to function during a catastrophic failure.

Cloud Service - The delivery of applications, systems, or infrastructure services over a network. Organizations can use cloud services as a way to utilize services from a service provider at a lower cost than the organization could achieve on its own.[1]

Confidentiality - The concept of information and functions being protected from unauthorized access and disclosure.[18] [19]

Cryptography - the science of hiding information in order to conceal it from unauthorized parties.

---

[18] Gregory, P. H. (2015). CISSP Guide to Security Essentials. Boston, MA, USA: Cengage Learning.

[19] For information about the legal requirements regarding confidentiality, see Appendix C: Legal Resources of this guide.

Cybersecurity - Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

Data Custodian - An employee who is responsible for the safe custody, transport, storage of the data and implementation of business rules for customer data.[20]

Denial of Service - A type of computer network attack where a malicious actor floods a firm's routers, switches, and other network devices with useless data in an effort to cripple or halt communications.

Device Access (Digital) - Any access to a device that is not gained through physical means.

Device Access (Physical) - Any access to a device that is physical.

Disaster Recovery Plan (DRP) - The practiced policies and procedures put into place to ensure a business is able to return to operations after a disaster has happened.

Domain - The formal name for a website address. It is typed into an internet browser (e.g., www.google.com).

Due Diligence - Due diligence generally describes the care a reasonable and prudent person must take to avoid harm to others or themselves.[21]

Encryption - The process of encoding a message so that only the intended parties are able to access that information.

External Risk - Any hazard that is external to the organization, which includes third party access. These risks are generally not controlled by the organization.

Firewall - A security system that monitors and controls computer network traffic.

Integrity - The concept of asserting that information may be changed only by authorized persons and means.

---

[20] Markiewicz, D. (2011, September 15). Information Roles and Responsibilities. Retrieved from https://www.cmu.edu/iso/governance/roles/docs/InformationSecurityRolesResponsibilities_FINALv1.0.pdf

[21] For more information regarding legal obligations for due diligence, see Appendix C: Legal Resources of this guide.

Internal Risk - Any hazard that is internalized to the organization, ranging from employees to technology and physical factors. These are risks that can usually be controlled by the organization.

Personally Identifiable Information (PII) - Generally, PII is defined as information that when used alone or with other relevant data can identify an individual.

Principle of Least Privilege - A policy that states that individuals should have access to only the systems, data, and functions that they require to perform their stated duties.[22]

Privacy - The control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.[23]

Privacy Breach - Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated.[24]

Proprietary Breach - Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated.[25]

Risk Assessment - The process of determining your organization's assets, be it physical or digital, and the risks that are associated with them and creating a policy that details the steps taken to mitigate, reduce, or transfer that risk.

Security Certificate - A document, signed by a trusted authority, that tells users that they are connected to a trusted, authentic website.

Software patches and updates - The periodic releases for software with the intent of fixing bugs or removing potential vulnerabilities.

TLS - Transport Layer Security, a method of encrypting electronic communication between two computers. This ensures that the connection is private. TLS is commonly used to secure web browsing and email communications.

---

[22] Gregory, P. H. (2015). CISSP Guide to Security Essentials. Boston, MA, USA: Cengage Learning.

[23] The Regents of the University of California, "Privacy and Confidentiality." Privacy and Confidentiality, 2015 https://www.research.uci.edu/compliance/human-research- protections/researchers/privacy-and- confidentiality.html

[24] United States, Congress, NIST. "Cybersecurity Framework." Cybersecurity Framework, 2014. www.nist.gov/cyberframework.

Third Party - Any outsourced or contracted party.

Two Factor Authentication - An extra layer of security that requires not only a username/password, but also a second piece of information that only the user has. (See: Authentication Credentials)

VPN - Virtual Private Network, a way to create a secure connection between two or more networks.

Wireshark - a network troubleshooting and analysis software tool. A passive monitor that collects local computer network traffic for later analysis.

Appendix B: Third Party Vendor Checklist

The following checklist developed by Covington & Burling LLP covers topics that may need to be discussed with a third party vendor. “Depending on the extent of the relationship and information that may be accessed by the vendor, the following areas of inquiry may be necessary to inform a cybersecurity diligence assessment:

- whether and how often the vendor has experienced cybersecurity incidents in the past, the severity of those incidents, and the quality of the vendor’s response
- whether the vendor maintains cybersecurity policies, such as whether the vendor has a written security policy or plan
- organizational considerations, such as whether the vendor maintains sufficient and appropriately trained personnel to protect the data and/or service at issue and respond to incidents
- human resources practices, particularly background screening employees, cybersecurity training, and the handling of terminations
- access controls, particularly whether controls are in place that restrict access to information and uniquely identify users such that access attempts can be monitored and reviewed
- encryption practices, including whether information is encrypted at rest, whether information transmitted to or from the vendor is properly encrypted, and whether cryptographic keys are properly managed
- evaluation of in what country any data will be stored
- the vendor’s policies regarding the secondary use of customer data, and whether IT systems are created in such a way as to respect limitations on secondary use
- physical security, including resilience and disaster recovery functions and the use of personnel and technology to prevent unauthorized physical access to facilities
- backup and recovery practices
- change control management, including protocols on the installation of and execution of software
- system acquisition, development, and maintenance to manage risk from software development or the deployment of new software or hardware
- risk management of the vendor’s own third-party vendors
- incident response plans, including whether evidence of an incident is collected and retained so as to be presentable to a court and whether the vendor periodically tests its response capabilities
- whether the vendor conducts regular, independent audits of its privacy and information security practices” (Fagan, et al)

Appendix C: Legal Resources

Introduction:

State licensed Investment Advisers and Investment Adviser Representatives have cybersecurity-related obligations under federal and state law, some of which are addressed by these Guidelines. This Appendix is intended to provide additional information on the obligations raised in the Guidelines, but it is not intended to be an exhaustive list of security and privacy obligations or to address any single obligation completely. Licensees must become familiar with the laws and rules that impact their operations.

In general terms, many of an Investment Adviser's cybersecurity obligations arise from the requirement under Maine's administrative rules to protect the security and confidentiality of the non-public personal information of any client. 02-032 C.M.R. ch. 515, § 14(19). Failure to take reasonable steps to achieve this protection is a violation of the rule.

More specific legal duties also exist, and the brief synopses below are intended only as an introduction to some of the relevant laws. When questions arise, the advice of legal counsel should be sought.

Terms:

Confidential Information - An Investment Adviser is asked in the Protect: Encryption section of these Guidelines to categorize data as confidential or non-confidential. The term "confidential information" is not defined in Ch. 515, but the rule states that the failure to "protect the security and confidentiality of the non-public personal information of any client" is a dishonest and unethical practice. Ch. 515 § 14(19). "Confidential information" may be understood to mean any client information that an Investment Adviser must keep private

Due Diligence - Due diligence generally describes the care a reasonable and prudent person must take to avoid harm to others or themselves. In the Protect: Cloud Services section of the Guidelines, due diligence describes the proper vetting of third-party providers, but due diligence should be applied to any number of actions an Investment Adviser may take to ensure adequate cybersecurity.

Personally Identifiable Information - Maine licensed Investment Advisers are required by 32 M.R.S.A. § 16411(9) to comply with the Gramm-Leach-Bliley Act and Regulation S-P. The Gramm-Leach-Bliley Act and Regulation S-P define "nonpublic personal information" as "personally identifiable financial information" and information about consumers derived from "personally identifiable financial information" that is not publicly available. 15 U.S.C. § 6809(4); 17 C.F.R. § 248.3(t).

Regulation S-P defines "personally identifiable financial information" as any information:

> (i) A consumer provides to obtain a financial product or service;
>
> (ii) About a consumer resulting from any transaction involving a financial product or service; or
>
> (iii) That is otherwise obtained about a consumer in connection with providing a financial product or service to that consumer.
>
> 17 C.F.R. § 248.3(u).

"Personally identifiable information" is not otherwise defined or used in the Maine Uniform Securities Act or in Ch. 515.

Investment Advisers should note that they may have obligations under Maine's Notice of Risk to Personal Data Act in the event of a data breach. Maine law, for purposes of obligations under the Notice of Risk to Personal Data Act, defines "personal information" as an individual's name in combination with one or more data elements, e.g., social security number, account number, etc., or a combination of data elements that would allow a person to fraudulently assume the identity of the person whose data was compromised. 10 M.R.S.A. § 1347(6).

Privacy - Failing to protect non-public personal information of any client is a dishonest and unethical practice under Ch. 515, §14(19).

The Maine Uniform Securities Act requires Investment Advisers licensed or required to be licensed in Maine to comply with the privacy provisions of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801, *et seq.*) and its implementing regulations, Regulation S-P (17 C.F.R. § 248.1 – 248.100). 32 M.R.S.A. § 16411(9).

Under the Gramm-Leach-Bliley Act, financial institutions, which includes Investment Advisers, have an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

Regulation S-P describes the conditions under which a financial institution may disclose nonpublic information to nonaffiliated third-parties. 17 C.F.R. §§ 248.3(n), 248.10.

Security Breach - Under Maine's Notice of Risk to Personal Data Act, a "Security Breach" means the unauthorized acquisition, release, or use of electronic data that includes personal information that compromises the security, confidentiality, or integrity of personal information. 10 M.R.S.A. § 1347.

In the event of a Security Breach, the person who maintains the data that includes personal information has obligations to investigate the likelihood that personal data has been or will be misused and to provide notice of the breach to affected Maine residents, credit reporting agencies, and, for Investment Advisers, the Maine Office of Securities. 10 M.R.S.A. § 1348.

Written Policies and Procedures - Ch. 515 § (7)(1)(Q) requires Investment Advisers to have "[w]ritten procedures to supervise the activities of employees and investment adviser representatives that are reasonably designed to achieve compliance with applicable securities laws and regulations." This is a broad mandate and should be applied to several aspects of cybersecurity. The Guidelines raise the following areas where written procedures are necessary: handling and use of electronic devices, terminating VPN access upon terminations, categorizing data as confidential or non-confidential, defining data security and/or encryption requirements, addressing the physical security of confidential data and systems containing confidential data, handling flagged network events, addressing a security incident, and storing and archiving information.

A critical component in preventing a potential Privacy Breach is ensuring that access to Personally Identifiable Information is limited solely to those individuals who require access to the information. Ch. 515 § 7(7)(C)(1) and (2) and Section 501 of the Gramm-Leach-Bliley Act [15 U.S.C. § 6801(b)] require the implementation of safeguards to limit access to a client's Personally Identifiable Information.

References

Fagan, D. N., Nigel, H. L., Wimmer K., Canter, E. H., Redmon, P. (2015, November 16). *Checklist: Pre-engagement due diligence when assessing third party cybersecurity risk.* Retrieved from https://www.securityroundtable.org/checklist-pre-engagement-due-diligence-when-assessing-third-party-cybersecurity-risk/

Federal Trade Commission. (2016, September). Data Breach Response: A Guide for Business. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

Gregory, P. H. (2015). CISSP Guide to Security Essentials. Boston, MA, USA: Cengage Learning.

Kissel, R., Regenschied, A., Scholl, M., Stine, K., Computer Security Division., Information Technology Laboratory. (2014, December). Guidelines for Media Sanitization. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Markiewicz, D. (2011, September 15). Information Roles and Responsibilities. Retrieved from https://www.cmu.edu/iso/governance/roles/docs/InformationSecurityRolesResponsibilities_FINALv1.0.pdf

North American Securities Administrators Association. (2017). NASAA Cybersecurity Checklist for Investment Advisers. Retrieved from http://nasaa.cdn.s3.amazonaws.com/wp-content/uploads/2011/08/NASAA-Cybersecurity-Checklist.pdf

Pusin, Y. (2015). The 3-2-1 Backup Strategy. Retrieved from https://www.backblaze.com/blog/the-3-2-1-backup-strategy/

The Regents of the University of California, “Privacy and Confidentiality.” Privacy and Confidentiality, 2015 https://www.research.uci.edu/compliance/human-research-protections/researchers/privacy-and-confidentiality.html

“Risk Assessment.” Risk Assessment | Ready.Gov, Department of Homeland Security, 2017, www.ready.gov/risk-assessment.

United States, Congress, NIST. “Cybersecurity Framework.” Cybersecurity Framework, 2014. www.nist.gov/cyberframework.

Acknowledgements

John Couch and Katrina Sabochick would like to thank Securities Administrator Judith M. Shaw, Director of Examination and Licensing Edward Moran, Securities Registration and Rulemaking Attorney James Liddell, and Senior Securities Examiners Andrew Shuman and Vanessa Smith of the Maine Office of Securities for giving us the opportunity to work with them on this guide, and for providing us with the legal resources to do so. We also could not have been granted this opportunity without assistance from former MCSC Director Raymond Albert. In addition, we would like to thank MCSC Director of Operations Lynn Lovewell and Director Henry Felch for their support and advice in writing this document.