ProCircular

SECURITY. PRIVACY. TRUST.

How RIAs Can Meet SEC Cybersecurity Requirements

Cybersecurity compliance requirements that registered investment advisors (RIAs) must follow to protect client data.

Whether you're with a large advisory firm or are a sole proprietor, financial and investment advisors in Iowa are now responsible for more than providing guidance and advice. In the shift to moving data and systems online, you now face information-security risks. As a result, the U.S. Securities and Exchange Commission (SEC) has created cybersecurity compliance requirements that registered investment advisors (RIAs) must follow to protect client data.

It's possible that your firm – regardless of size – could be audited by the SEC for compliance with these requirements. If this happens, they'll be looking for signs of established policies, appropriate roles, assessment of potential vulnerabilities, correction of possible security flaws, and creation of response plans in case a cybersecurity incident were to occur.

Conducted in late 2016, a TD Ameritrade survey involving 1,000+ financial/investment advisors revealed that only 18% are "very confident" they could pass a cybersecurity exam conducted by the SEC's Office of Compliance Inspections and Examinations.

Your clients trust you with very important, private information. It's your responsibility to keep it safe, and out of the hands of unauthorized users. Are you doing everything you can to safeguard their private information?

Why Cybersecurity Matters

Depending on the scope, a breach could be overwhelming to a financial/investment advisory firm. And it could happen in many different ways:

- **Phishing**, where an unknown source encourages an employee or client to download an unsafe attachment or click on an unsafe link
- **Unauthorized access** to web portals that combine client data (such as bank, credit card, retirement, and investment account information)
- **An unencrypted email** sent from an advisor to a client (or vice versa) containing sensitive information that is intercepted

Although they may not be asking specific questions yet, it won't be long before potential clients (and existing customers) start asking how you'll protect their data. This conversation should be part of onboarding new clients – and reviewed regularly with established customers.

If data is compromised, your client's first reaction may be to terminate the relationship. That reaction can be avoided when you have a plan and the appropriate resources in place to mitigate and recover from a breach. Taking preventative and preparatory steps ahead of time can also improve the likelihood of collecting on your insurance policy if you are hacked.

Here, we've summarized the six areas that the SEC cybersecurity requirements focus on – and what you should be doing to comply. Seem overwhelming? Don't worry – you can handle it! Keep reading to the end, and we'll show you how.

1. Regular Cybersecurity Risk Assessments

Assess the following on a regular basis:

- Cybersecurity policies and procedures for handling customer information
- Potential internal and external cybersecurity threats
- Security controls and processes, including penetration testing and vulnerability assessments
- Plans for next steps after a breach

A good way to document these assessments is to include them in board minutes or meeting agendas —that will serve as proof that you're regularly examining your cybersecurity status and discussing risks and incident response and planning. This is also a good place to document the results of penetration testing and vulnerability assessments, as well as the actions taken to correct issues that are uncovered.

2. Access Control

Who can access your client files, data, and records? Individual employee access privileges must be determined and maintained. (For example: Does your receptionist or HR director really need full access to all customer information?) Any time there is a personnel or system change, these access privileges should be revisited.

According to the SEC, you must have basic controls, policies, and procedures in place to prevent unauthorized personnel and third parties from accessing data and devices. Controls can include things like multifactor authentication, user-credentials management and authorization, firewalls and other perimeter defenses, and tiered employee access to sensitive information.

There should be policies and procedures in place regarding login attempts and failures, lockouts, and unlocks/resets, including how often systems are reviewed to check for failed and unauthorized login attempts (signaling potential trouble). There should also be guidelines to follow about how and when system notifications are shared with customers and employees.

Simple solutions that include two-factor authentication can be used to greatly improve your situation as well. While there may be a week-long struggle to get everyone familiar with how to make it work, once it's in place, access will be locked down significantly.

Typical in most office environments, BYOD (bring your own device) has permeated financial advisor workplaces. Make sure you have basic procedures in place detailing if and when personal devices can be used to access company/customer data, and document how those devices will be secured. The capability to monitor, track, and deactivate should be possible with company-issued devices; common systems like Office365 have made this much easier than in years past.

3. Data Loss

Systems and tools should be in place to prevent, detect, and monitor the loss of client data, as well as policies and procedures related to monitoring external distribution of sensitive information (through email, U.S. mail, document-transfer tools, etc.). Software that can monitor technology systems for unauthorized intrusions, data loss, or other unusual events is available.

When thinking about data loss prevention, you should be able to answer questions like:

- How are you controlling content transferred outside your firm (whether through employees or through third parties)?
- How do you verify the authenticity of a request to transfer customer funds?
- Are you using data encryption to communicate personal information?
- Are you restricting the use of transportable storage media (such as flash drives)?
- Are methods in place to make sure that software and applications are frequently updated, and security patches are installed?
- What process do you follow to dispose of records with private information once you no longer need them?
- What are the plans for data backup (and retrieval in case of data loss)?

4. Vendor Management

Just as important as the cybersecurity practices you follow are the cybersecurity practices that *your third-party vendors follow*—especially the vendors who have access to your clients' sensitive information. Make sure proper access controls are in place regarding vendor access to your network, software, and/or data.

5. Training

Employees may unknowingly be putting your firm's data at risk. Something as simple as losing a smartphone or downloading an attachment from an unknown source can open the door to trouble. Proper training, however, can turn your employees into a great first line of defense. Teach them how and when to alert appropriate parties about suspicious activity, and make sure they follow protocol when accessing and transferring client data.

Provide regular education about data security and risks. This training should be documented – including who participated, what they learned, and when/where the training occurred – and available for employees to review at any time.

Offering client and third-party vendor training may be a good idea, too, to help remind customers and partners why it's important to follow appropriate guidelines when creating passwords, sharing login information, reporting unauthorized transactions, etc.

6. Incident Response

If a breach occurs, what would your next step be? Who would you contact? How would you handle damage control? Establishing an incident response plan ensures business continuity, and can help mitigate the effects of a cybersecurity incident. Once a plan is in place, it should also be tested and reviewed periodically so any necessary adjustments can be made.

Clear policies and procedures should be documented and communicated with clients to cover things like how losses due to unauthorized activity will be covered.

It's also a good idea to have plans to share with clients about what they can do to protect themselves: monitoring credit reports, changing passwords/pins, and alerting financial and credit card institutions.

What Step Should I Take Next?

Depending on the size of your firm, and the capabilities of in-house IT staff, you may be able to tackle several of these cybersecurity initiatives on your own.

For peace of mind and to help reduce risk, however, it's a good idea to bring in an outside party to take an up-close look at internal and external controls, identify any security gaps, and help you prioritize potential fixes based on your budget and current exposure level.

When possible, ProCircular recommends working with a local cybersecurity firm. Having a trusted partner nearby means you'll be able to develop close working relationships with key people who will grow to understand the way your firm works, the challenges it faces, and the budget you need to abide by. And if an incident occurs, a local firm is just a few miles away and can be onsite within minutes to help investigate and alleviate the damage.

Essentials
ReadySecure™
by ProCircular

ProCircular just unveiled a new cybersecurity solution designed to help you meet SEC cybersecurity requirements. ReadySecure™ is a reasonably priced subscription package that can help you meet the RIA SEC requirements, keep your clients' data safe, and protect your reputation.

Everything you need is wrapped up in one simple package:

- Quarterly internal/external vulnerability assessments
- On-demand anti-phishing testing for employees
- CyberBlock threat monitoring
- Yearly incident response planning
- Yearly risk assessments
- Security policy library
- Monthly cybersecurity newsletter and informational updates to share with staff

With ReadySecure, you can spend less time worrying about securing client data and more time focusing on managing their investments and providing sound financial advice.

To learn more, visit www.procircular.com/readysecure.