



Agile Advisors, Strong Partnerships:

How Advisors Can Meet Evolving Cybersecurity Mandates

THE CYBERSECURITY LANDSCAPE IS EVOLVING - HOW ARE YOU KEEPING UP?

Cybersecurity continues to be of significant importance for Investment Advisors and clients. Even the smallest cybersecurity incident can result in investors losing money, firms losing business, or the heavy weight of sanctions, fines and negative headlines.

As firms increasingly turn to compliance partners to provide top-tier service to their clients, the risks they're encountering are also evolving. With frequent hacking attempts, brute force password cracking, and even AI-enhanced deep fakes, firms are all too aware of the need for up-to-date protocols and software.

Moreover, the SEC requires firms to not only implement information security safeguards but also disclose material cybersecurity incidents, among other things. These rules are ultimately designed to both protect consumer confidence in our industry and strengthen our ability to secure client data.



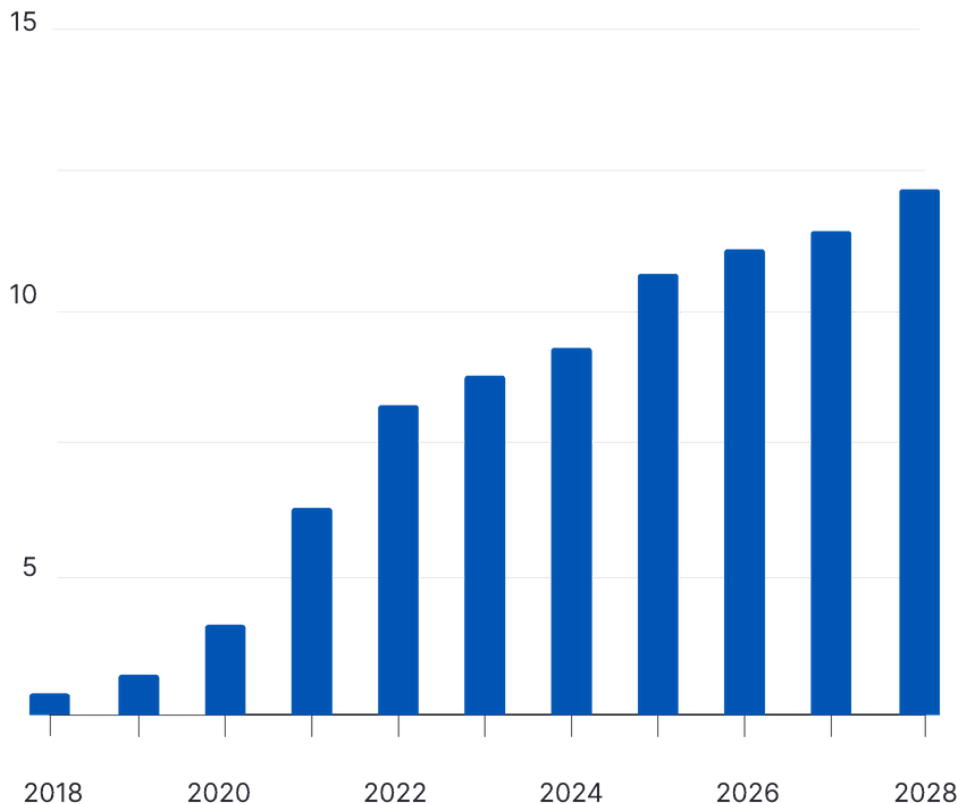
THE STATE OF RIA CYBERSECURITY RISK MANAGEMENT

The SEC's current rules under the Investment Advisers Act of 1940 require RIAs to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks, disclose information about cybersecurity risks and incidents, report information confidentially to the SEC about certain cybersecurity incidents, and maintain related cybersecurity records.

Firms need to be vigilant in their approach to cybersecurity. Of course, with the right compliance partner., staying up-to-date is relatively easy. Adapting to evolving rules and regulations is table-stakes, and yet many RIAs are struggling to meet constantly shifting demands from regulators. Firm leadership should regularly assess their cybersecurity, data security and workflow risks, while assessing whether they're adequately disclosing their cybersecurity practices to clients. Some firms are capable of bringing these functions in-house, but most firms will need assistance understanding, integrating, and complying with new requirements.

CYBERCRIME EXPECTED TO SKYROCKET

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)



As of Sept. 2023. Data shown is using current exchange rates.
Source: Statista Market Insights

THE HEAVY WEIGHT OF A CYBER INCIDENT

The SEC is tackling a wide range of topics, including steps for mitigating business risks and personal damage from cyberattacks, enhancing data privacy, mandating robust technical controls and strengthening record maintenance.



Business Risks

Firms that lack the proper cybersecurity protocols face significant risks. Firms that are victims of hacks, data breaches or other cyber incidents can incur financial losses as a result of regulatory fines and lawsuits, lost revenue, lost clients, recovery costs and higher insurance premiums. They may also suffer reputational damages, due to mandated disclosures. Incidents can also disrupt a firm's operations, leading to inefficiencies from company personnel leaving the firm.



Personal Damage

It's not unusual to hear about the emotional cost of a cyberattack from advisors, clients or executives who have been victims of a cyberattack. Business owners might find it difficult to sleep, as they focus on a response and repairing damage done to their business. Employees are often unsure if data has been exposed, or worry that they'll lose their job due to a company's financial losses. Clients naturally fear that they will experience financial loss of their own.



Data Privacy

The SEC already requires firms to implement an identity theft program, but putting a data loss prevention protocol in place is crucial for protecting and preserving data privacy. Confidential or identifying information might be used to steal an individual's identity, or be used to impersonate, threaten them, blackmail them or publicly disclose private information. In the age of AI-enabled deep fakes, protecting data becomes all the more critical.



Technical Controls

Like an immune system, firm-wide cybersecurity is composed of a number of interconnected pieces and parts. Technical controls help firms maintain data privacy and manage risks by defining who gets access to what, for how long and in what manner. The SEC expects firms to have policies in place for identity and access management; mobile device management; software patches and updates; identifying, evaluating, documenting and mitigating network and software weaknesses; data loss prevention; cybersecurity risk assessments and cyber awareness training.



Record Maintenance

The SEC requires several record-keeping requirements for books and necessary documents, governing what is retained and for how long. Firms should retain a copy of their cybersecurity policies and procedures for five years, including written reports documenting their annual review of policies and procedures. Good record keeping also entails documenting occurrences, if any, of cybersecurity incidents, including responses and recovery over the previous five years. Firms should also retain cybersecurity risk assessments from the last five years.

FIND THE OVERLAP BETWEEN COMPLIANCE AND SECURITY

It's important that firms also understand the difference between compliance and cybersecurity, so that they can operate where those elements overlap. Firms can be compliant—adhering to industry regulations—without developing a secure investing or business environment. Conversely, it's possible to create a secure work environment, albeit one that's outside the bounds of compliance.

The key is to operate where the two concepts overlap. Regulation-aware cybersecurity is a set of practices and processes designed to safeguard data and systems from adversaries and bad actors and, at the same time, meet regulatory requirements.

Advisory firms that leverage their compliance platforms to support an overarching cybersecurity plan are best geared for success. While navigating the complexities of cybersecurity processes and protocols can be time-consuming and overwhelming, missing the mark would be devastating if an incident were to occur. By partnering with the right compliance platform, future crises may be averted.



Learn more about Smartria's cybersecurity compliance strategies and solutions.

SCHEDULE A DEMO