CHECKLIST

SEC Cybersecurity Recommendations for Registered Investment Advisors (RIAs) and Investment Companies

September 2023

Introduction

Since 2011, the Security Exchange Commission (SEC) has taken a distinct focus on cybersecurity stance of Registered Investment Advisors (RIAs) and investment companies ("funds") to adopt stronger cybersecurity programs and policies.

On July 26, 2023, the Securities and Exchange Commission (SEC) issued **final rule documentation** that requires publicly traded companies to provide enhanced and standardized disclosures regarding cybersecurity risk management, strategy, governance, and incident disclosure. These newly adopted rules address concerns over investor access to timely and consistent information related to cybersecurity, and specifically look to enhance and standardize disclosures regarding:

- Material cybersecurity incidents, which need to be disclosed within four business days of being deemed material.
- New disclosure requirements for cybersecurity risk management and strategy, management's role in assessing and managing material risks from cybersecurity threats, and the board of directors' oversight of cybersecurity risks.

Now, the SEC is shifting their focus to RIAs and funds. In October 2023, the SEC is expected to release the Final Rule proposed under the Investment Advisers Act of 1940 and the Investment Company Act of 1940 that will require RIAs and funds to better address their cyber risks, enable 24/7 threat detection and response capabilities, and disclose significant cybersecurity incidents in a timely manner.

In addition, the SEC is also pushing for more transparency around cybersecurity incident disclosure, **noting that** they're "concerned that clients and investors may not be receiving sufficient cybersecurity-related information…to assess the operational risk at a firm or the effects of an incident to help ensure they are making informed investment decisions".

As a result, the goal of this proposed rule is to address four key areas of cyber risk management: risk assessment, threat and vulnerability management, cybersecurity incident response and recovery, and user security and access.

Moving forward, we anticipate that the SEC will follow with guidance to further structure and solidify their requirements surrounding incident response, resilience, and survivability. To that point we've updated this cybersecurity recommendations documentation as a resource guide based on the newly adopted rules.

Pragmatic Security Matrix

In response to the new guidance from the SEC, we've identified several elements that make up this year's updated Pragmatic Security Matrix that are categorized into several pillars:

1. Risk Governance and Oversight
2. Risk Assessments
3. Cybersecurity Technical Controls
4. Incident Response – Management and Resilience
5. External Dependency Management/Vendor Due Diligence
6. Security Awareness Training
7. Threat Intelligence and Information Sharing

These specific measures don't necessarily create an explicit list for what firms should be doing to fulfill their duties regarding information security. As a result, based on your firm's assets under management (AUM), we've created a pragmatic recommendations matrix to help your team develop the right cybersecurity program.

Of course, these recommendations may vary depending on your firm's domicile(s), number of employees, technical maturity, regulatory requirements, and strategy.

	Risk Governance and Oversight	Risk Assessments	Cybersecurity Technical Controls	Incident Response – Management and Resilience	External Dependency Management/ Vendor Due Diligence	Security Awareness Training	Threat Intelligence and Information Sharing
Take an inventory of all security components and infrastructure	✓	✓	✓	✓	✓		
Formalize and document identity strategies (Authentication, Authorization, Accounting)	✓		✓				
Document security defense mechanisms from a "Kill Chain" perspective.	✓	✓	✓	✓	✓		
Document, implement, and test Incident Response strategies	✓	✓	✓	✓	✓	✓	
Implement employee phishing and security awareness training efforts						✓	✓
Define acceptable RPO/RTO given a focus on resilience	✓		✓	✓			

Risk Assessment

The first step in designing effective cybersecurity policies and procedures is assessing and understanding the cybersecurity risks facing an adviser or a fund. As an element of an adviser's or fund's reasonable policies and procedures, the proposed cybersecurity risk management rules would require advisers and funds periodically to assess, categorize, prioritize, and draft written documentation of, the cybersecurity risks associated with their information systems and the information residing therein.

The proposed cybersecurity risk management rules would require advisers and funds, when conducting this risk assessment, to:

(i) Categorize and prioritize cybersecurity risks based on an inventory of the components of their information systems, the information residing therein, and the potential effect of a cybersecurity incident on the advisers and funds; and

(ii) Identify their service providers that receive, maintain or process adviser or fund information, or that are permitted to access their information systems, including the information residing therein, and identify the cybersecurity risks associated with the use of these service providers.

The proposed rules would also require written documentation of any risk assessment. Generally, this risk assessment should inform senior officers at the adviser or the fund of the risks specific to the firm and support responses to cybersecurity risks by identifying cybersecurity threats to information systems that, if compromised, could result in significant cybersecurity incidents.

Firms with AUM < 1b	Firms with 1b - 5b AUM	Firms with AUM > 5b
✓ Recognize and identify what data is held within the company itself and by third parties (those responsible). Pay particular attention to PII (for both clients and employees) and financial information.	✓ Enact a Zero-Trust Identity strategy.	✓ Complete the NIST Cybersecurity Framework document.
✓ Ensure that data is only available to those who need it (including viewing, copying, modifying, etc.).	✓ Read through the NIST Cybersecurity Framework document to gain familiarity with it.	✓ Regularly (e.g., weekly) perform filesystem scans for Personally Identifiable Information (PII).
✓ Use encryption where it's deemed most effective (especially for externally facing purposes).	✓ Document defense measures in place within the Kill Chain Response Matrix.	✓ Document critical data flows between the firm and third-parties.
✓ Ensure data is backed up regularly and securely (and that restores are tested on a regular basis). Ensure that RTO/RPO are well-defined.	✓ Regularly (e.g., monthly) perform filesystem scans for Personally Identifiable Information (PII).	✓ Segregate different areas and data sources (e.g., using tiered access and/or network segregation).
✓ Require proof from third-party vendors that they are addressing cybersecurity concerns. Confirm details for most critical vendors.	✓ Regularly perform (e.g., monthly) vulnerability scans from Internal, External, Wireless, Network and WebApp perspectives.	✓ Participate in FS-ISAC meetings to keep up-to-date with cyberthreats and vulnerabilities.
✓ Ensure that contracts with external vendors consider cybersecurity risk (with language included).	✓ Regularly perform (e.g., monthly) vulnerability assessment of user access/privileges/permissions.	✓ Review newest capabilities of security providers.
✓ Ensure that continuous external and internal vulnerability assessments are performed.		
✓ Join affiliate bodies such as the Hedge Fund Tech Connect (HFTC) to gain broader knowledge in the field.		
✓ Complete the Security Program Maturity Assessment (SPMA) and Security Incident Response Planning (SIRP) engagements.		
✓ Ensure that annual penetration testing is performed.		
✓ Re-certify users' access rights on a periodic basis (including users, administrators, and service accounts).		

Threat and Vulnerability Management

Detecting, mitigating, and remediating threats and vulnerabilities is essential to preventing cyber incidents before they occur. Advisers and funds generally should seek to detect cybersecurity threats and vulnerabilities through ongoing monitoring (e.g., comprehensive examinations and risk management processes).

Ongoing monitoring of vulnerabilities could include, for example, conducting network, system, and application vulnerability assessments. This could include scans or reviews of internal systems, externally-facing systems, new systems, and systems used by service providers. Advisers and funds generally should also monitor industry and government sources for new threat and vulnerability information that may assist them in detecting cybersecurity threats and vulnerabilities.

In general, once a threat or vulnerability is identified, advisers and funds should consider how to mitigate and remediate the threat or vulnerability, with a view towards minimizing the window of opportunity for attackers to exploit vulnerable hardware and software. Methods for mitigating and remediating threats and vulnerabilities could include, for example, implementing a patch management program to ensure timely patching of hardware and software vulnerabilities and maintaining a process to track and address reports of vulnerabilities.

An adviser or a fund should adopt policies and procedures that establish accountability for handling vulnerability reports, and processes for intake, assignment, escalation, remediation, and remediation testing.

Firms with AUM < 1b	Firms with 1b - 5b AUM	Firms with AUM > 5b
✓ Use well-established and effective Endpoint Detection and Response security solutions. ✓ Ensure that data is only available to those who need it. ✓ Enforce a rigorous password policy for all systems and users. Two-factor authentication should be considered for external access, remote access, and privileged access. ✓ Restrict Local Administrator credentials (e.g., investigate Microsoft LAPS). ✓ Ensure that all patching is up to date including servers, workstations, firewalls and network equipment. Higher priority must be placed on systems with data/services most at-risk and those with external access available. ✓ Log all system login accesses for diagnostic and/or forensic use should an incident occur. ✓ Enforce physical security within the office space. ✓ Restrict access to critical data through selective privilege mapping/user management. ✓ Restrict removable storage usage (e.g., USB keys, writable media). ✓ Regularly (e.g., weekly) review all critical data files accessed. ✓ Create an incident response plan that is tested at least annually. ✓ Conduct continuous External, Internal and Webapp vulnerability assessments. ✓ Ensure that annual penetration testing is performed. ✓ Conduct regular cybersecurity training and phishing tests. ✓ Document all assets prioritizing critical assets to the organization.	✓ Incorporate the components of a cyber resilient security program, including continuous monitoring, threat intelligence and 24/7 threat detection and response capabilities. ✓ Regularly (e.g., daily) review all critical system login/access failures. ✓ Complete **eSentire Pragmatic Security Event Management** process and test strategies annually at a minimum. ✓ Consider the use of enhanced encryption at rest for critical data. ✓ Track efficacy of cybersecurity solutions (e.g., EDR). ✓ Consider two-factor authentication on all system access as part of a Zero-Trust framework.	✓ Consider code assessments of all in-house code. ✓ Incorporate vulnerability scanning into the development pipeline if applicable. ✓ Conduct physical penetration testing.

Cybersecurity Incident Response and Recovery

As an element of an adviser's or fund's reasonable policies and procedures, the proposed cybersecurity risk management rules would require advisers and funds to have measures to detect, respond to, and recover from a cybersecurity incident. These include policies and procedures that are reasonably designed to ensure:

I. Continued operations of the fund or adviser;

II. The protection of adviser information systems and the fund or adviser information residing therein;

III. External and internal cybersecurity incident information sharing and communications; and

IV. Reporting of significant cybersecurity incidents to the Commission.

Finally, the proposed rules would require advisers and funds to prepare written documentation of any cybersecurity incident, including their response and recovery from such an incident.

Cybersecurity incidents can lead to significant business disruptions, including losing the ability to communicate or the ability to access accounts or investments. These incidents also can lead to the unauthorized access or use of adviser or fund information. Having policies and procedures reasonably designed to respond to cybersecurity incidents can help mitigate these significant business disruptions. A cybersecurity program with a clear incident response plan designed to ensure continued operational capability, and the protection of, and access to, sensitive information and data, even if an adviser or fund loses access to its systems, would assist in mitigating the effects of a cybersecurity incident. Advisers and funds, therefore, may wish to consider maintaining physical copies of their incident response plans—and other cybersecurity policies and procedures—to help ensure they can be accessed and implemented during the times they may be needed most.

We believe it is critical for advisers and funds to focus on operational capability, including resiliency and capacity of information systems, so that they can continue to provide services to their clients and investors when facing disruptions resulting from cybersecurity incidents. The ability to recover critical systems or technologies, including those provided by service providers, in a timeframe that meets business requirements, is important to mitigate the consequences of cybersecurity incidents. An adviser or fund may consider implementing safeguards, such as backing up data, which can help facilitate a prompt recovery to allow an adviser or fund to resume operations following a cybersecurity incident that leads to the unauthorized access or use of adviser or fund information.

An incident response plan should also designate adviser or fund personnel to perform specific roles in the case of a cybersecurity incident. This would entail identifying and/or hiring personnel or third parties who have the requisite cybersecurity and recovery expertise (or are able to coordinate effectively with outside experts) as well as identifying personnel who should be kept informed throughout the response and recovery process. In addition, an incident response plan should generally have a clear escalation protocol to ensure that an adviser's and fund's senior officers, including appropriate legal and compliance personnel, and a fund's board (as applicable) receive necessary information regarding cybersecurity incidents on a timely basis.

Moreover, under proposed rule 204-6 and amendments to Form ADV Part 2A, as well as amendments to funds' disclosure requirements, advisers and funds would have to report any significant cybersecurity incidents to the Commission and make appropriate disclosures to their clients and investors. Accordingly, advisers and funds must include provisions in their policies and procedures designed to ensure their compliance with their reporting and disclosure obligations as part of their cybersecurity incident response.

Advisers and funds should also consider testing their incident response plans to assess their efficacy and to determine whether any changes are necessary, for example, through tabletop or full-scale exercises. As part of the annual review of their policies and procedures, advisers and funds are required to review and assess the design and effectiveness of the policies and procedures and should generally consider amendments to correct any identified weaknesses in their design or effectiveness.

Firms with AUM < 1b	Firms with 1b - 5b AUM	Firms with AUM > 5b
✓ Log all system login accesses for diagnostic and/or forensic use should an incident occur. ✓ Restrict removable storage usage (e.g., USB keys, writable media). ✓ Review and complete eSentire Incident Response Framework document or similar Incident Response preparation collateral. ✓ Regularly (e.g., weekly) review all critical data files accessed. ✓ Test backups on a regular cadence to ensure they work as intended.	✓ Regularly (e.g., daily) review all critical system login/access failures. ✓ Complete **eSentire Pragmatic Security Event Management** process and test strategies annually at a minimum. ✓ Complete a Business Continuity/Disaster Recovery Plan and test strategies at least annually.	✓ Test portions of Business Continuity/Disaster Recovery and Incident Response strategies quarterly and perform full tests on an annual basis. ✓ Consider the use of Data Loss Prevention technology.

User Security and Access

As an element of an adviser's or fund's reasonably designed policies and procedures, the proposed cybersecurity risk management rules would require controls designed to minimize user-related risks and prevent the unauthorized access to information and systems.

Their policies and procedures must include:

1) Requiring standards of behavior for individuals authorized to access adviser or fund information systems and any adviser or fund information residing therein, such as an acceptable use policy;

2) Identifying and authenticating individual users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification;

3) Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;

4) Restricting access to specific adviser or fund information systems or components thereof and adviser or fund information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the adviser or fund; and

5) Securing remote access technologies used to interface with adviser or fund information systems.

The proposed cybersecurity risk management rules would require advisers and funds, as part of their cybersecurity programs, to address user access controls to restrict system and data access to authorized users.

Firms with AUM < 1b	Firms with 1b - 5b AUM	Firms with AUM > 5b
✓ Ensure that data is only available to those who need it. ✓ Enforce a rigorous password policy for all systems and users. two-factor authentication should be considered for external access. ✓ Restrict Local Administrator credentials (e.g., investigate Microsoft LAPS). ✓ Log all system login accesses for diagnostic and/or forensic use should an incident occur. ✓ Enforce physical security within the office space. ✓ Restrict access to critical data through selective privilege mapping/user management. ✓ Restrict removable storage usage (e.g., USB keys, writable media). ✓ Regularly (e.g., weekly) review all critical data files accessed.	✓ Regularly (e.g., daily) review all critical system login/access failures. ✓ Complete **eSentire Pragmatic Security Event Management** process and test strategies annually at a minimum. ✓ Consider the use of enhanced encryption at rest for critical data. ✓ Consider two-factor authentication on all system access as part of a Zero-Trust framework.	✓ Consider code assessments of all in-house code.

Build Resilience & Prevent Disruption with eSentire

Our cybersecurity services portfolio is designed to build cyber resilience, so your business can effectively anticipate, withstand, and recover from even the most advanced cyberattacks.

We provide 24/7 threat protection that is proactive, personalised and cost-effective.

Our powerful cloud-native, open eSentire XDR Platform ingests network, cloud, log, endpoint and identity signals, correlating indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes.

Our Cyber Resilience Team, comprised of 24/7 SOC Cyber Analysts, Elite Threat Hunters, Threat Response Unit (TRU), and your named Cyber Risk Advisor, acts as an expert extension of your team to investigate, contain and stop threats that have the potential to bypass automated security controls.

ANTICIPATE

Exposure Management Services

Strategic services including Vulnerability Management, vCISO and Managed Phishing & Security Awareness Training to identify gaps, build defencive strategies, operationalise risk mitigation and continuously advance your security program.

WITHSTAND

Managed Detection & Response

We deliver Response + Remediation you can trust. By combining our cutting-edge XDR platform, 24/7 threat hunting and security operations leadership, we hunt and disrupt known and unknown threats before they impact your business.

RECOVER

Incident Response & Digital Forensics

Battle-tested Incident Commander level expertise, crime scene reconstruction and digital forensics investigations that can bear scrutiny in a court of law. The world's fastest threat suppression with a 4-hour SLA available with our IR Retainer.

Ready to Get Started?

Reach out to connect with an eSentire security specialist and build a more resilient security operation today.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US (1)866-579-2200

eSentire

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organisations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organisation's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.