ECI

NEW SEC RULES FOR CYBERSECURITY RISK MANAGEMENT

How investment advisers and funds should respond today.

CONTENTS

NEW CYBERSECURITY RULES FOR A CHANGING THREAT LANDSCAPE

The SEC believes cyber risk has a bearing on all aspects of its three-part mission: to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation.

With that in mind, the agency has established new rules around cyber risk management for investment advisers and funds. The rules are designed to improve cybersecurity preparedness and increase investor confidence. While in the past the SEC has focused more on recommendations and best practices, now the agency has shifted its stance to implementing a prescriptive ruleset and creating accountability.

At the highest level the rules require advisers and funds to implement written cybersecurity policies and procedures, disclose significant cyber incidents to the SEC and clients, and maintain cybersecurity records.

They also establish best practices for protecting data, controlling data access, managing threats and vulnerabilities, responding to cyber incidents, and establishing cybersecurity accountability. The move follows sanctioning of eight firms in August 2021 for failures in their cybersecurity policies and procedures – clear evidence the SEC is taking cybersecurity enforcement seriously.

There's a lot to unpack in the 224-page SEC document that delineates the new rules. But the takeaway is that investment advisers and funds must take specific actions around seven core aspects of cyber risk management: policies and procedures, access management, data protection, vulnerability management, incident response, reporting, and accountability (see Figure on page 6).

With the rules first proposed in 2022 set to be finalized without change in spring 2023, the time to take action is now. Addressing all aspects of the directives isn't something your firm will achieve overnight. However, the good news is that the new SEC rules represent best practices for safeguarding your information assets from cyberattack – and should be implemented regardless of whether the SEC requires them. Following the recommendations here will help you achieve compliance, secure your business against disruption, and help build trust with regulators and clients.

ACTION 1

ESTABLISH WRITTEN CYBERSECURITY PLANS, POLICIES AND PROCEDURES

Most organizations maintain some type of guidelines that govern their cybersecurity. Now, the SEC wants firms to review and formalize their cyber risk plans, policies and procedures in detailed, written documents that establish workflows, responsibilities, and accountability.

This is a cybersecurity best practice, because your plans, policies and procedures form the basis of all your cybersecurity efforts. These documents should be comprehensive to cover all aspects of your business. The SEC will require that you keep them easily retrievable for two years and archived for five.

Start by assessing, categorizing, and prioritizing your unique cyber risks and aligning cybersecurity with your specific business model. For instance, if you rely on trading algorithms, the SEC expects you to have policies and procedures around secure application development.

Next, identify and classify your business-critical information architecture and data assets. Firms often overlook this step, but it's crucial to document your IT environment and understand where your data resides – especially investor data. It's the only way to be sure you're securing that data on an ongoing basis.

That includes identifying service providers that have access to your data. You might outsource an IT platform or service, but you're still responsible for protecting the data involved. You also must be able to sustain processes investors rely on – even if you have to do it manually – if service-provider systems go down.

Finally, understand that cyber threats and IT infrastructures change over time. So, make sure cyber policies and procedures remain relevant and up to date. Review formalized documents at least annually. If you make a substantial change to your environment – such as migrating to the cloud – update policies and procedures accordingly.

"Plans, policies and procedures provide a foundation for your cybersecurity framework. They need to be comprehensive to cover all aspects of your business."

- Rich Itri, Chief Innovation Officer, ECI

KEY TAKEAWAYS: CYBERSECURITY PLANS, POLICIES AND PROCEDURES

Document a robust cyber risk plan.

Assess, categorize, and prioritize your unique risks.

Identify critical service providers that have access to your data.

Make sure documentation is easily retrievable.

Formalize your cybersecurity policies and procedures.

Classify your datasets.

Review policies and procedures at least annually.

Update based on business changes that could affect cyber risk.

ACTION 2

REVIEW, DOCUMENT AND ENFORCE ACCESS MANAGEMENT BEST PRACTICES

In the past, the SEC has offered suggestions for how to manage data access. Now, it's being highly specific about what comprises best practices for access management. In fact, access management is the most prescriptive aspect of the new SEC rules.

It begins with Acceptable Use Policy (AUP), a document that stipulates behaviors and constraints users agree to in order to access data. It continues with timely management of credentials during onboarding, offboarding, and at the start and end of projects. In short, be sure to terminate credentials whenever they're no longer needed.

A related necessity is least-privilege access, in which users have permissions to use only the information resources they require to do their jobs. This calls for a clear understanding of your systems, SaaS Platforms, and your data. Cybersecurity tools can help but getting a handle on least-privilege access can take months, so the time to begin is now. The SEC will also require "a combination of two or more credentials for access verification." That approach doesn't necessarily represent strong authentication, because two or more credentials could be a username, a password and a pet's name, which is essentially just a longer password.

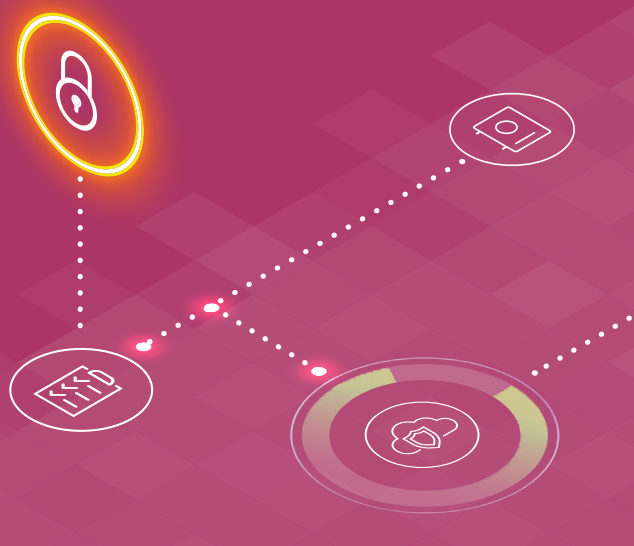
What the SEC appears to be calling for is Multi-Factor Authentication (MFA), now considered a cybersecurity necessity. True MFA combines what you know (a password), what you have (a device) and what you are (a biometric such as a fingerprint). The SEC also wants firms to understand their network perimeter.

That used to be the four walls of your office. But with cloud computing, Software as a Service (SaaS) and a remote workforce, your perimeter is in constant flux. Cyber solutions such as a Cloud Access Security Broker (CASB) – a tool that monitors user activity and enforces security policies – can help.

In fact, securing remote access is a specific SEC requirement. That doesn't apply just to employees. Contractors, partners, vendors and other third parties also require security techniques like MFA. Don't neglect strong authentication for processes like wire transfers – a common oversight.

"The SEC is becoming much more prescriptive about cybersecurity approaches such as acceptable use policy, least-privilege access and multifactor authentication."

- Bill Tan, Chief Information Security Officer, ECI



KEY TAKEAWAYS: CYBERSECURITY PLANS, POLICIES AND PROCEDURES

Best practices for data access management are now SEC policy.

Implement multifactor authentication (MFA).

Create and enforce an acceptable use policy (AUP).

Closely involve IT for access management, device management, endpoint protection, and training.

Create policies for passwords, least-privilege access, and remote access.

Review and update policies regularly.

ACTION 3

DEPLOY DATA PROTECTION POLICIES AND TECHNOLOGIES

The SEC has laid out specific parameters for monitoring and protecting data from unauthorized access.

The goal is to maintain data confidentiality, integrity, and availability – for both data at rest and data in transit.That will require a careful inventory of data and a clear understanding of where it resides – knowledge many organizations lack. Do you maintain data in a datacenter? Across multiple cloud environments? In Dropbox or on Google Drive? In email? On vendor systems? Understanding your data landscape will enable you to protect it effectively – and allow you to communicate to regulators and clients whether data has remained protected.

> **"Even if your data resides on vendor systems, you still have an obligation to inform clients and partners if any of that data was potentially breached."**
>
> - Steve Schwartz, Director, Security Consulting, ECI

The new SEC rules also prescribe technologies and methodologies for protecting data. These include:

SEGMENTATION

Segregate datacentres, cloud environments, and networks to keep data separate based on sensitivity level or value to business continuity.

VULNERABILITY MANAGEMENT

Leverage vulnerability assessment and remediation to uncover malware, backdoors, hosts communicating with botnet-infected systems, and webservices linking to malicious content.

MOBILE DEVICE MANAGEMENT

Avail yourself of tools or services to ensure proper device configuration, restrict sensitive data from devices, and remotely wipe devices when necessary.

ACCESS CONTROLS

Employ tools and best-practice methodologies to manage data access.

DATA ENCRYPTION

Encrypt data while at rest on hard drives and while in motion over networks.

THREAT DETECTION AND PREVENTION

Deploy automated tools and services – including security information and event management (SIEM) based on machine learning (ML) and statistical analysis – to detect and prevent threats.

USER TRAINING

Make sure employees are well-versed in managing passwords, recognizing and responding to phishing attacks, and other basics of cyber hygiene. Training services can help. Finally, the SEC wants firms to understand and document vendors and partners who might have access to data. You should contractually require vendors to meet minimum cybersecurity standards and to promptly report cyber incidents. If a vendor system is penetrated, you have an obligation to report to clients which of your data has been affected.

KEY TAKEAWAYS: DATA PROTECTION POLICIES AND TECHNOLOGIES

Monitor and protect data from unauthorized access.

Leverage methods such as encryption, network segmentation, access controls and automated threat detection.

Safeguard data based on sensitivity level and importance to operations.

Document which vendors have access to data.

Protect data when it's stored and as it's transmitted.

Require vendors to meet cybersecurity standards and report cyber incidents.

ACTION 4

MANAGE THREATS AND VULNERABILITIES

For the first time, the SEC is setting the expectation that firms should deploy technology to continuously monitor their IT environments for threats and vulnerabilities. This is a significant development.

SEVEN KEY ASPECTS OF NEW SEC CYBERSECURITY RULES

Many firms lack an integrated platform for monitoring, alerting about, responding to, and remediating cyberattacks. They might use piecemeal solutions that address some of these needs in some contexts. But many don't currently address threats and vulnerabilities in the comprehensive fashion the SEC has called for. In addition to implementing robust technology tools, you need established processes for taking action based on the insights those solutions provide. And you need to test those processes to ensure they'll function as desired when remediation is necessary.

You should conduct regular vulnerability scans and penetration tests to identify cyber risks and update applications with security patches to protect against zero-day threats. Note that vulnerability management covers not just security patches but also hardware and software configuration. Make sure security services in your cloud environments are turned on as appropriate. Remember: it's not enough simply to have policies for vulnerability and threat management. You also need to demonstrate to regulators and clients that prescribed processes are being followed.

> **"For the first time, the SEC requires that firms have sufficient technology for cybersecurity monitoring and management of their environment."**
>
> - Rich Itri, Chief Innovation Officer, ECI

KEY TAKEAWAYS: CYBERSECURITY PLANS, POLICIES AND PROCEDURES

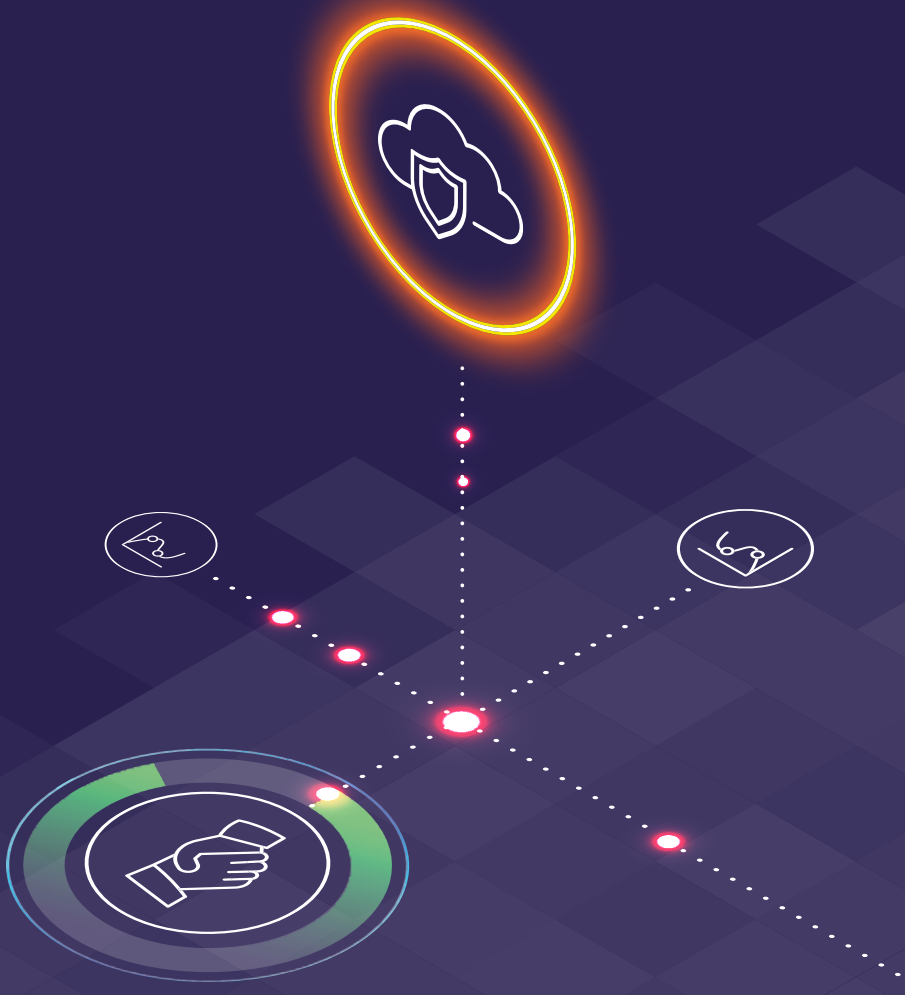
Perform regular vulnerability scans.

Track, prioritize and remediate known vulnerabilities.

Update and patch software promptly.

Don’t overlook device and application configuration.

Conduct regular penetration tests.



ACTION 5

IMPLEMENT CYBERSECURITY INCIDENT RESPONSE PLANNING AND RECOVERY

The National Institute of Standards and Technology (NIST) has established a cybersecurity framework that includes five core functions: identify, protect, detect, respond and recover.

While the SEC isn't requiring firms to adopt the framework, it does use NIST language in its rulemaking. Firms should become familiar with the NIST guidelines and consult it as they develop their cyber policies. In setting out rules for response to and recovery from cyber incidents, the SEC focuses on the last three NIST functions.

Specifically, the agency will "require advisers and funds to have measures to detect, respond to and recover from a cybersecurity incident," as follows:

DETECT

You can no longer rely on piecemeal solutions for threat detection. Rather, you need a comprehensive platform to detect and respond to incidents in near real time. An effective SIEM solution will leverage artificial intelligence (AI) to filter out the noise and home in on anomalous signals that requires attention.

RESPOND

Your response plan will differ depending on your unique risks and business requirements. But you need a playbook for responding to common cyber events, from stolen laptops to a business email compromises to ransomware attacks. A playbook will help you avoid the shortcomings of ad hoc response and escalation, specifying clear roles, responsibilities, and procedures. Conduct tabletop exercises, with clear response metrics, to fine-tune your playbook so that you're prepared when the inevitable cyber incident occurs.

RECOVER

Rapid and complete recovery is essential for sustaining business continuity and maintaining regulator and client confidence. This is an area where it pays to consult a trusted cybersecurity partner. An experienced cyber expert has fine-tuned recovery processes through real-world experiences with many firms. Consider carefully whether you want to go it alone and must learn from mistakes that could negatively impact your business.

Finally, if you outsource any IT platforms or data services to a vendor, you should be able to continue operations even if their systems are interrupted by a cyber event. Start by documenting service providers that have access to your data. Then make sure you have procedures for handling data on an alternative system or briefly sustaining processes manually. The goal is to maintain business continuity regardless of where your data resides.

KEY TAKEAWAYS: CYBER INCIDENT RESPONSE PLANNING AND RECOVERY

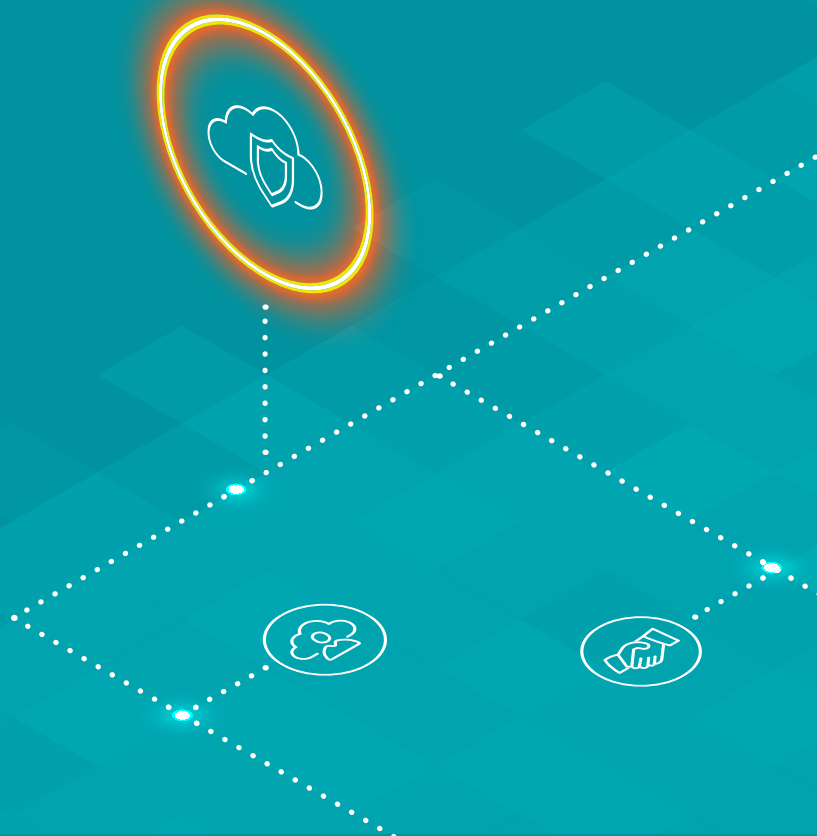
Develop and document an incident response plan and recovery procedure.

Include metrics for speed and effectiveness of response.

Test the response plan and fine-tune it based on results.

Identify ways to handle data if vendor systems become unavailable.

> "The SEC strongly suggests that firms should build their incident response around the guidelines and best practices in the NIST cybersecurity framework."
>
> - Bill Tan, Chief Information Security Officer, ECI



ACTION 6

REPORT AND DISCLOSE CYBERSECURITY INCIDENTS

Reporting of cyber incidents used to be a gray area for the SEC. If a cyber event didn't appear to be directly detrimental to clients, firms weren't required to report it. With the new rulemaking, that has changed. Firms will now have to report to the SEC and disclose to clients any "significant" cyber incident.

The SEC defines a significant incident as **"any cyber event that results in substantial harm or disruption of critical operations for the adviser or its clients."** This is one of the most consequential elements of the SEC rules, as it calls for a level of transparency and process the SEC hasn't specifically required before.

Reportable cyber incidents can be grouped in two broad categories. One involves the interruption of critical operations. The other involves the exposure of confidential information such as customer data, employee data or business intelligence.

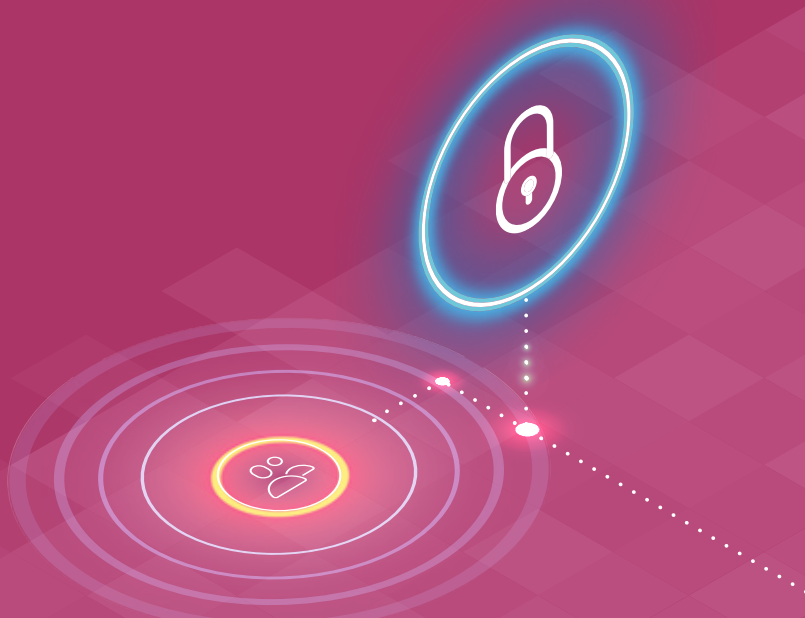
Reporting of the event must occur within 48 hours of discovery. That means you'll need a detailed and tested process, with clear roles and responsibilities, so you can report promptly and accurately.

In fact, reporting should be part of your broader incident response plan. You should document who will lead the response and which team members will perform which response actions. You should also have a process for reporting to not only the SEC but also your local FBI office as well as your board of directors.

Reporting to the SEC will be handled through a confidential process. But the SEC will also require that firms publicly disclose both cyber risks and cyber incidents to clients and the SEC in brochures and registration statements. Disclosures must cover any incident that occurred in the preceding two fiscal years.

"The SEC will require that boards of directors be made aware of any data breaches and any changes to your environment that occur as a result of those breaches."

- Steve Schwartz, Director, Security Consulting, ECI

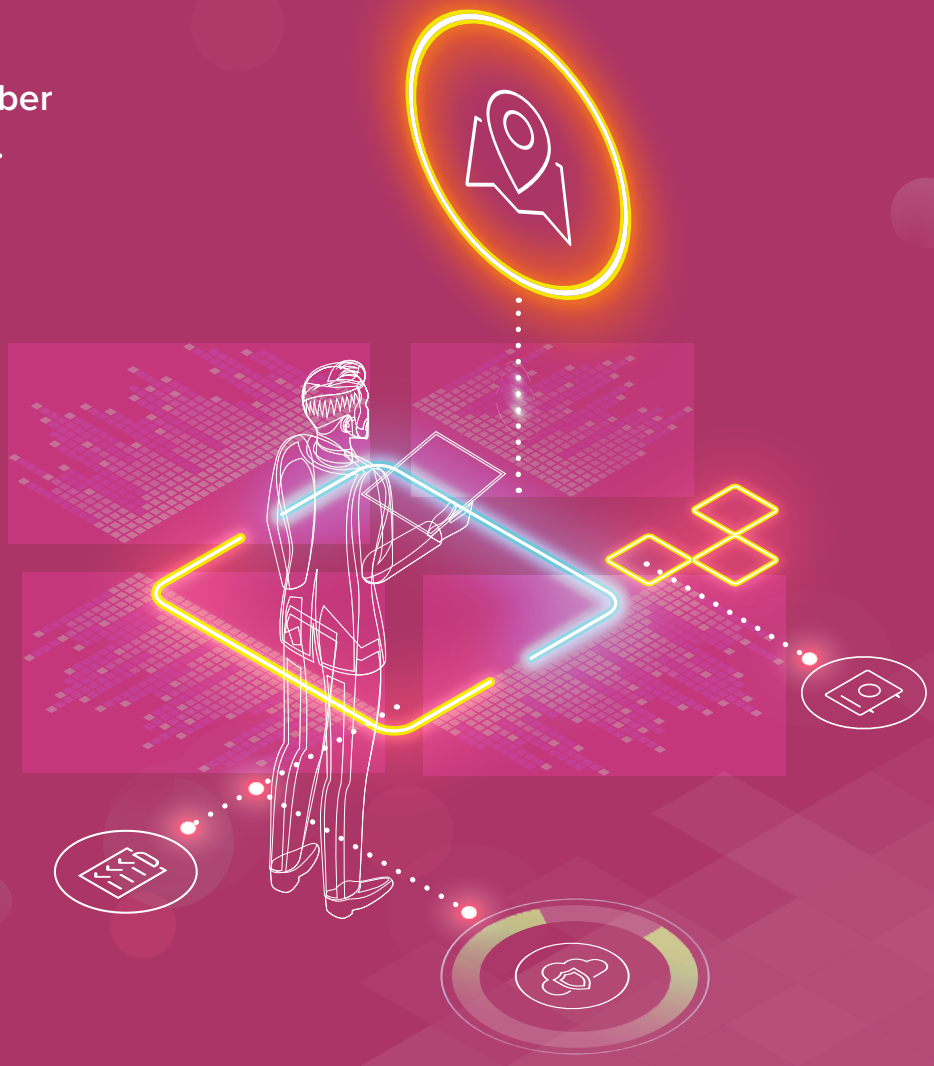


KEY TAKEAWAYS: CYBER INCIDENT REPORTING AND DISCLOSURE

Reporting of cyber incidents is a major new SEC requirement that calls for a new level of transparency.

Publicly disclose cyber risks and incidents from the previous two fiscal years to both clients and the SEC.

Report significant cyber incidents to the SEC.



ACTION 7

FORMALIZE CYBERSECURITY RESPONSIBILITY AND ACCOUNTABILITY

A key goal of the new SEC rulemaking is to strengthen responsibility and accountability for cyber risk management. This accountability extends to your board of directors. And for good reason, because the best way to create accountability throughout an organization is to establish the right tone at the top.

Your board must now review and approve all cyber-related policies and procedures. It should also accept ultimate responsibility for the health of your cyber program. That will force implementation and maintenance of your cyber framework across the firm.

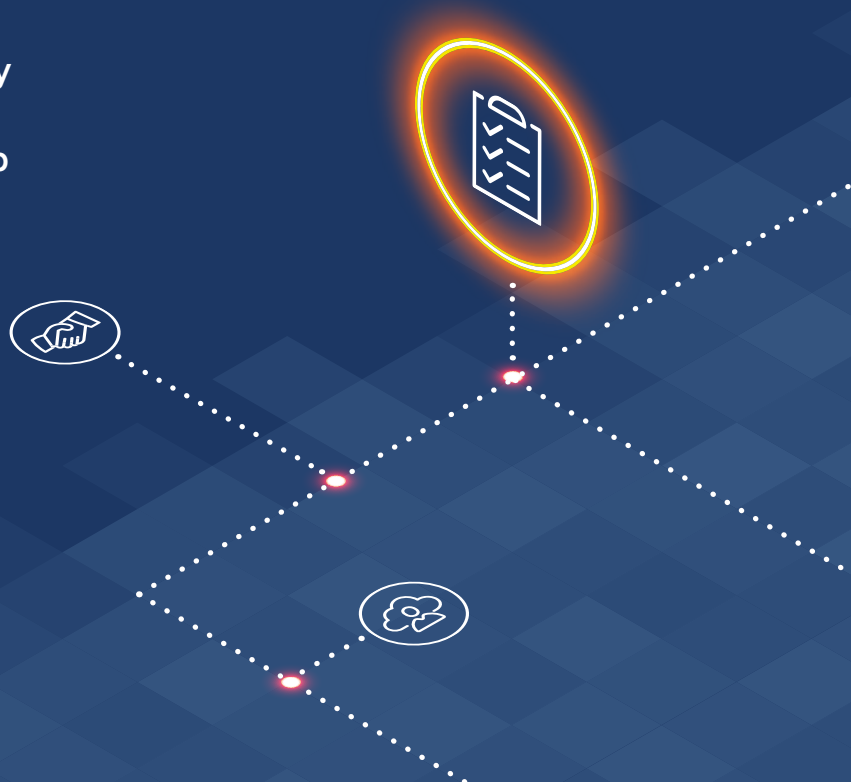
A key enabler of board accountability is a procedure to promptly inform the board of cyber incidents. Equally important is a process to keep the board apprised of your cybersecurity posture, including vendors that handle firm data.

Establish metrics for cyber risk management, measure against them, and report to the board in a clear, consumable manner on a monthly, quarterly, and annual basis. While budgetary support for such a process might have been limited in the past, the new SEC rules should drive funding to ensure it happens.

Your board will also be responsible for understanding the cyber risks that exist in your market and the best practices for addressing them. This is a new level of engagement that not all boards will be prepared for. Work with your board members to bring them up to speed.

"The SEC now requires accountability for cybersecurity. The best way to achieve that is to establish ownership at the top of the organization."

- Rich Itri, Chief Innovation Officer, ECI



KEY TAKEAWAYS: CYBERSECURITY RESPONSIBILITY AND ACCOUNTABILITY

New SEC rules formalize cybersecurity accountability.

Boards of director must review and approve cybersecurity policies and procedures.

Boards must also understand and address cyber threats in the marketplace.

Alert boards to cyber incidents.

Inform boards about vendors that handle sensitive data.

TAKING ACTION TO MANAGE CYBER RISK

With its new rules for cybersecurity risk management, the SEC is effectively formalizing cybersecurity best practices as policy. The agency is charging investment advisers and funds with clear requirements to mitigate against cyberattacks and report cyber incidents as they occur.

It will become imperative for you to identify, protect against, and mitigate cyber risk in a more focused and formal way. You'll need to identify your information assets both inside and outside your network, understand your workflows and vulnerabilities, and deploy effective technologies and methodologies to reinforce your cybersecurity posture.

In effect, the SEC is enforcing what many organizations already know are today's cybersecurity imperatives. But firms will no longer be able to relegate responsibility or delay adoption. Taking action to comply with the new SEC rules, strengthen cyber programs, and reinforce client trust will take time, focus and effort. **The time to begin is now.**

NEW SEC RULES FOR CYBERSECURITY RISK MANAGEMENT

The SEC's new rules for cybersecurity risk management, set to be finalized on April 2023, can be encapsulated in these seven actions for investment advisers and funds:

1. Establish written cybersecurity plans, policies and procedures.
2. Review, document and enforce access management best practices.
3. Deploy data protection policies and technologies.
4. Manage threats and vulnerabilities.
5. Implement cybersecurity incident response planning and recovery.
6. Report and disclose cybersecurity incidents.
7. Formalize cybersecurity responsibility and accountability.

Ready to take your cybersecurity beyond lights on?

Contact ECI today for assured business acceleration through technology.

800.752.1382. | eci.com

ABOUT ECI

ECI is the leading provider of managed services, cybersecurity and digital transformation for alternative financial services organizations across the globe. With its unmatched platform of solutions, ECI provides assured business acceleration through technology, partnering with clients to drive innovation. More than 1,000 customers worldwide with over $3 trillion of assets under management put their trust in ECI.

US: +1 800 752 1382

UK: +44 207 071 6802

Singapore: +65 6622 2345

Hong Kong: +852 3189 0101

For more information visit: **www.eci.com**