PROPOSED SEC CYBERSECURITY REPORTING REQUIREMENTS

Everything You Need to Know

Last year, the Securities and Exchange Commission (SEC) proposed new rules to enhance and standardize cybersecurity risk management, strategy, governance, and incident reporting disclosure practices by public companies and other market entities. The proposed rules could have a sweeping impact on all public companies that are subject to the Securities Exchange Act of 1934. Let's take a closer look at what the proposed rules include.

Incident Reporting

The proposed rules would require public companies to disclose information about a material cybersecurity incident within four business days after determining an incident occurred. This includes information such as when the incident was discovered, whether it has been resolved, what the scope of the incident includes, and whether or not any data was compromised as a result of the incident. Companies will also be required to provide updates on previously disclosed cybersecurity incidents.

But what constitutes a material incident? According to the SEC, "information is defined as material if there is a substantial likelihood that a reasonable shareholder would consider it important in an investment decision."

When determining the materiality of an incident, public companies will need to consider:

- **Whether or not data was compromised;**
- **Whether or not the company's policies and procedures were violated;**
- **Whether or not access to data changed following the incident;**
- **Whether or not a malicious actor gained access to data, threatened the organization, and/or demanded payment.**

To determine whether an incident is material or not, BARR recommends working with a dedicated cybersecurity partner to assist with the potential disclosure.

.

Risk Management, Strategy, and Governance Disclosure

In addition to requiring incident reporting, the proposed rules will also require public companies to periodically report on their risk management, strategy, and governance. This includes reporting on the company's cybersecurity policies and procedures, the role of management on implementing said policies and procedures, and cybersecurity expertise at the board level.

The Reasoning

Given the financial impact that cybersecurity risks and incidents can have, the proposed rules are intended to allow investors in a publicly traded company to understand the company's risk management, strategy, and cybersecurity practices and better inform their investment decisions.

"Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks. A lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner," stated SEC Chair Gary Genslinger.

How BARR Can Help

All public companies should be actively preparing for the proposed rules, which may come with challenges, such as struggling to understand what constitutes a material incident, difficulty communicating cybersecurity impacts at the board level, and having dedicated roles for cybersecurity risk management. That's where BARR comes in—BARR's team of cybersecurity experts can address these challenges and more.

On the consulting side of our practice, BARR's cybersecurity consultants can partner with companies to provide strategic guidance on complying with the proposed rules. Our experts can help companies draft the necessary disclosures on incidents, risk management, strategy, and governance. In the event of a cybersecurity incident, BARR consultants will help organizations determine the materiality of the incident and provide guidance so that a company can make an informed decision about how to proceed. Furthermore, our specialists can also help companies communicate the impact of cybersecurity risks to their board of directors.

Partnering with BARR may be particularly helpful to smaller public companies without the dedicated teams to manage cybersecurity disclosures. For companies that may need an attestation over the objectives of the ruling, BARR's attest team can perform a necessary audit to ensure compliance.

BARR ADVISORY

Contact Us

Have questions about the proposed SEC reporting requirements and how to prepare? Contact BARR today.

About BARR Advisory

BARR Advisory is a cloud-based security and compliance solutions provider specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud Platform. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Compliance Services**
  [HIPAA/HITRUST]
- **ISO 27001 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Cybersecurity Consulting and vCISO Services**
- **Compliance Program Assistance**

Connect with BARR

Want to learn more about how BARR's suite of services can benefit your organization?

Contact us today, or visit our **content library** to learn more.