BITSIGHT

GLASS LEWIS

WHITE PAPER

The SEC's New Cybersecurity Regulations

Part II: How should Shareholders Evaluate Company Cybersecurity Practices?

Table of Contents

Cybersecurity can impact financial performance **04**

What does the new SEC regulation require companies to disclose? **05**

Leveraging analytics to understand a company's cybersecurity posture **07**

Cyber incident disclosure and questions of materiality **09**

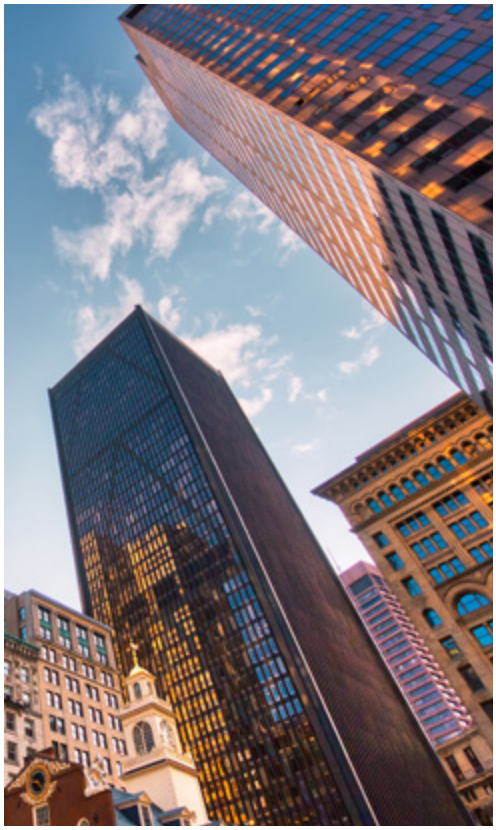
THE SEC'S NEW CYBERSECURITY REGULATIONS

What Shareholders Should Know

It seems everyone is concerned about cybersecurity these days, and the investor community is no different. Shareholders are reading the headlines—ransomware attacks, data breaches, infrastructure disruptions—and they are wondering how these incidents could impact the companies that they invest in.

Shareholders are about to get a lot more information from companies in the months ahead. In July 2023, the U.S. Securities and Exchange Commission (SEC) adopted new cybersecurity disclosure requirements that are designed to provide shareholders with enhanced information to help them understand how companies are addressing cybersecurity risks.

In this new era of transparency and accountability, how can shareholders leverage cybersecurity information in their investment decisions and corporate engagement strategies? In Part II of our series on cybersecurity, we'll discuss a few key issues for shareholders:



- **Is cybersecurity a material financial risk?**
- **How should shareholders evaluate the cybersecurity of companies they invest in?**
- **What should shareholders expect from disclosures?**
- **What are important indicators that a company's cybersecurity program is performing well... or not?**

> "
>
> Shareholders are about to get a lot more information from companies in the months ahead

Please note that this guide is for informational purposes only. It does not constitute legal advice, and you should consult with your own counsel about the specific application of these new rules to your organization.

01. Cybersecurity can impact financial performance

First things first—is cybersecurity really a material issue for investors? The answer is a resounding "yes."

Cybersecurity performance is a governance indicator that is a positive indicator of company performance and a negative indicator of downside risk. Research shows that poor cybersecurity can have a negative impact on share price. In recent years, various researchers have demonstrated that significant cybersecurity incidents can cause material declines in both share price and market share. These analyses are based on reviewing publicly disclosed breaches and tracking share price post-breach. Credit ratings services firm Moody's frequently warns that cyber incidents can be credit negative for affected companies and sectors.

But cybersecurity should not just be viewed by shareholders as an investment risk. Research also demonstrates that ongoing, strong cybersecurity performance is also linked to higher valuations. Well-performing companies were demonstrated to actually outperform a benchmark index by approximately 1% to 2% with lower volatility. In certain sectors, such as U.S. Technology, well-rated companies outperform the benchmark by 7%.

In other words, cybersecurity represents both risk and opportunity for shareholders. It has never been more important for shareholders to understand how the companies that they invest in are approaching cyber risk management. Now that the new SEC regulation is in effect, what should they do?

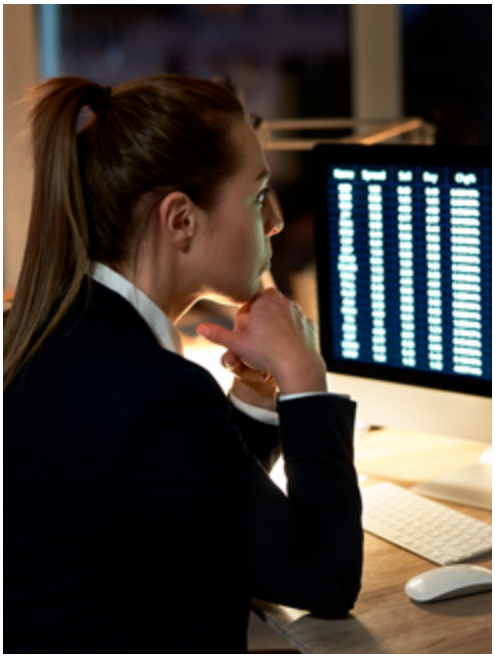
> "
>
> Cybersecurity represents both risk and opportunity for shareholders..

02. What does the new SEC regulation require companies to disclose?

Shareholders can anticipate learning more from public companies about their cybersecurity programs and performance in the months ahead. The SEC's cybersecurity regulation creates new obligations for public companies to report "material" cybersecurity incidents and require more detailed disclosure of cybersecurity risk management, expertise, and governance. Companies are required to disclose risks in their annual reports beginning on December 15, 2023.

The SEC's cybersecurity regulation will require disclosure in three main areas:

- First, the SEC requires organizations to describe the company's processes for assessment, identification, and management of material risks from cybersecurity threats in its Form 10-K.
- Second, organizations must describe the board's oversight of risks from cybersecurity threats and management's role in assessing and managing material risks from cybersecurity threats in its Form 10-K.
- Third, the SEC requires disclosure of any material cybersecurity incident in Form 8-K within four business days of determining that an event is material.



Many companies have, in practice, disclosed cybersecurity information (usually as a "risk factor") in various SEC filings over the years. For example, in a 2022 analysis of Fortune 100 company disclosures, the EY Center for Board Matters found that 99% of companies referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures and systems; 66% referenced response readiness, such as planning, disaster recovery or business continuity considerations; and 88% disclosed that at least one board-level committee was charged with oversight of cybersecurity matters. In the months ahead, we can expect more specific information about management and board efforts from all publicly traded companies, not just the Fortune 100.

And we might expect to see new kinds of information disclosure outside of the standard practices. While the SEC is intentionally vague in its regulatory requirements, there is a wide range of information that shareholders should be looking for when it comes to understanding and evaluating cybersecurity governance. For example, shareholders should ensure they understand:

- The organization's overall cybersecurity strategy, including the company's approach to addressing third party cyber risk management
- The organization's use of recognized frameworks to assess its risk (ex: NIST Cybersecurity Framework)
- Overall management organizational structure (e.g. organizational chart, roles/responsibilities, reporting structures, qualification and background of key leaders and management)
- Overall board of directors oversight (board committee charters, expertise of board members in cybersecurity issues, frequency of interaction with management, metrics used to evaluate effectiveness, use of third party advisor experts, etc.)
- Organization's overall investment in cybersecurity, including the level of resources to cybersecurity measures (including areas like technology investment, threat monitoring, employee training, etc.)
- Key policy and technical controls used to manage risk from threats
- Independent third party security evaluations, including SOC 2 certifications and cybersecurity ratings
- Measurements and metrics to determine effectiveness of the cybersecurity program, including industry benchmarks
- Incident management procedures, including frequency of tabletop exercises and executive-level involvement
- Cyber insurance coverage
- Approach used by the organization to understand financial risk arising from cyber risk and incident impact
- A "Materiality Methodology" utilized by the organization to provide insight and assurance to investors about how the company arrives at its materiality determination in the cybersecurity context

Shareholders should expect to see more granular information disclosed in annual filings. And while the SEC requires cybersecurity disclosure in Forms 10-K and 8-K, shareholders should also look to other types of investor reports for this critical information—including sustainability reports, ESG reports, shareholder presentations, and even standalone cybersecurity reports designed for the shareholder audience. We believe that many companies will continue to communicate critical governance and risk oversight in these types of investor reports.

03. Leveraging analytics to understand a company's cybersecurity posture

Beyond reviewing cybersecurity governance information, how will shareholders know that the cybersecurity program is actually working? Many shareholders do not have deep expertise in cybersecurity technology or risk. They need data and information that is understandable, comparable, reliable, and decision-useful.

> "Bitsight's data is not only useful as a risk screen. Independent analysis has found that investors leveraging Bitsight Security Ratings in an investment strategy can earn higher returns while reducing risk.

Fortunately, shareholders do not have to rely solely on information disclosed by companies in order to gain insight into the effectiveness of their cybersecurity programs. Glass Lewis is partnering with Bitsight to help shareholders obtain quantitative, objective data to better understand a company's cybersecurity posture. This data is valuable for shareholders who want timely, meaningful, and actionable information about cybersecurity from the companies that they invest in.

In 2011, Bitsight created the world's first cybersecurity rating system and has since partnered with many of the world's leading organizations serving investors including Glass Lewis and Moody's to improve investor and market awareness of cyber risks. Today, thousands of investors, enterprises, insurers, government institutions and other market stakeholders trust Bitsight's independent ratings and data to make better risk management decisions.

Bitsight continuously and non-intrusively collects cybersecurity performance data about public and private companies. Using this data, Bitsight creates quantitative, objective ratings and analytics that are similar to credit scores and updated daily. Independent studies show that Bitsight's ratings and analytics are significantly correlated with cybersecurity incidents. Poor cybersecurity performance as measured by Bitsight increased an organization's risk of experiencing a cybersecurity incident.

Glass Lewis is leveraging the cybersecurity expertise of Bitsight to provide investors insight into the level of cyber risk that a company is exposed to. Glass Lewis Proxy Papers feature a point in time snapshot of a public company's cybersecurity performance, pulled directly from the Bitsight platform. The report features the company's overall Bitsight Security Rating and how the organization benchmarks against its peers, the organization's performance over the last 12 months, the likelihood of ransomware incidents, the likelihood of data breach incidents, and any publicly disclosed incidents in the last 18 months. .

Investors can use Bitsight to manage cyber risk to their portfolios and help with engagement strategy. Bitsight's cybersecurity analytics help investors assess the effectiveness of the policies, controls, governance and procedures that a company is implementing, providing investors greater visibility into how well the cyber risk program is being executed. Bitsight's measurements also provide investors with further validation of management's intentions. Shareholders play a pivotal role in holding companies accountable for safeguarding their investments from cyber threats, and Bitsight data is ideal to leverage in an engagement strategy.

> "There is a wide range of information that shareholders should be looking for when it comes to understanding and evaluating cybersecurity governance.

With the Bitsight cybersecurity report in Glass Lewis Proxy Papers, investors get a comprehensive and accessible overview of key portfolio risks and opportunities integrated directly into their proxy voting and stewardship.

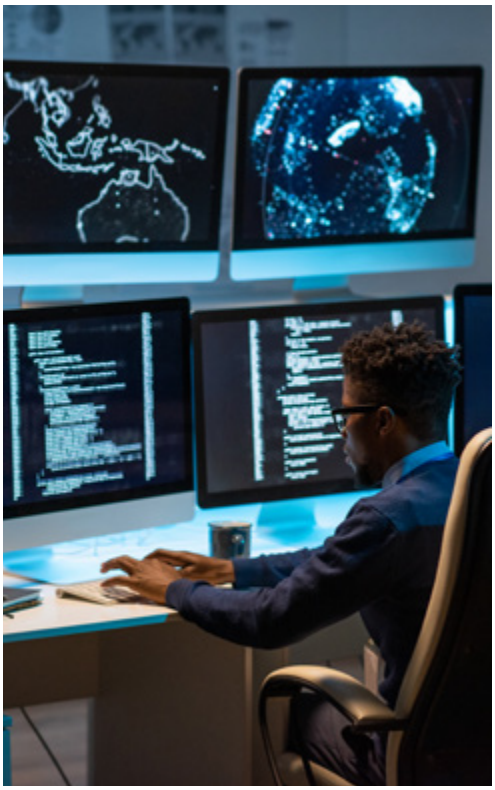
Bitsight's data is not only useful as a risk screen. Independent analysis has found that investors leveraging Bitsight Security Ratings in an investment strategy can earn higher returns while reducing risk.

04. Cyber incident disclosure and questions of materiality

Shareholders should pay particular attention to the way that companies develop guidelines around cybersecurity incident materiality determinations. In a discussion of the final rulemaking, the SEC described inconsistencies in registrant efforts to effectively disclose material incidents, which essentially caused the development of the new cybersecurity regulation.

What exactly is a material cybersecurity incident? According to the SEC, understanding whether a cybersecurity incident is material requires a company to analyze the total mix of quantitative and qualitative data surrounding the incident. There is not a specific financial threshold for a material cyber incident. In fact, the SEC states in the regulation, "...some cybersecurity incidents may be material yet not cross a particular financial threshold."

The SEC offers a few examples of what a material cybersecurity incident might look like. "For example, an incident that results in significant reputational harm to a registrant may not be readily quantifiable and therefore may not cross a particular quantitative threshold, but it should nonetheless be reported if the reputational harm is material. Similarly, whereas a cybersecurity incident that results in the theft of information may not be deemed material based on quantitative financial measures alone, it may in fact be material given the impact to the registrant that results from the scope or nature of harm to individuals, customers, or others, and therefore may need to be disclosed."



Because cybersecurity incident disclosure is such an important topic—and can lead to a decline in financial performance and stock price—shareholders should seek information about the methodology that organizations use to determine materiality in the context of a cybersecurity incident.

Gain a deeper understanding of your company's cyber risk profile through our exclusive partner solution from industry leader Bitsight.

Next steps

New SEC regulations have taken the topic of cybersecurity beyond the boardroom and directly to investors.
Is your company fully aware of its cybersecurity risks and the potential impacts on your stakeholders?

Glass Lewis' cybersecurity risk evaluation connects you with a Bitsight representative. This personalized session explores the critical areas of your cyber risk profile and provides guidance on how your company can enhance its cybersecurity. It's never been more critical to understand your cybersecurity risk.

Are you interested in learning more?

Don't hesitate to reach out →

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT