BITSIGHT

DATA SHEET

Cybersecurity Regulatory Reporting

What you need to know about the SEC's new cybersecurity regulations

Quick facts:

All publicly traded companies in the US

Disclose cybersecurity process, governance incidents and risk in 10Ks and 8K

Effective December 15th, 2023

The U.S. Securities and Exchange Commission (SEC) recently adopted new cybersecurity requirements for publicly traded companies. The new rules create obligations for reporting "material" cybersecurity incidents and requiring detailed disclosure of cybersecurity risk management, expertise, and governance. Companies are required to disclose risks in their annual reports beginning December 15, 2023.

There are three core components of the new SEC Cybersecurity Requirement:

1. Disclose material cybersecurity incident in Form 8-K within four business days
2. Describe the roles of executives and the Board of Directors in cyber risk management and oversight
3. Describe processes for assessing, identifying, and managing risks from cybersecurity threats in Form 10-K

Is this really new?

Yes and no. While cybersecurity risk reporting is new to the SEC, companies have been disclosing cybersecurity risk, oversight, and governance to investors in a variety of forums for years.

There are more than one hundred examples of companies publicly disclosing their Bitsight Security Rating or information about their Bitsight measurements as a means for communicating risk and building confidence in cybersecurity programs.

Where to start?

Communicating cybersecurity risk to non-cybersecurity investors and boards can be challenging. What security leaders often find is that the easiest, most intuitive starting point is to benchmark your risk against peers in your industry.

As an example, Equifax notes that its security capabilities "ranked in the top 1% of Technology companies and top 3% of Financial Services companies analyzed."

Cybersecurity Disclosure Examples

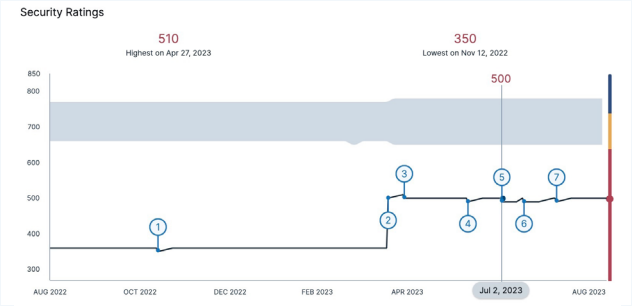
- **Darling Ingredients** leverages cybersecurity performance benchmarks in its Annual ESG Report, describing its cyber program as "being in the top 10% of the Energy/Resource Industry."
- **Schneider Electric** includes cybersecurity performance benchmarks in its Annual Sustainability Report, describing its program as being ranked "in the Top 25% in external ratings for Cybersecurity performance."

Peer Comparison

Benchmarking and objective insights to communicate cybersecurity risk.

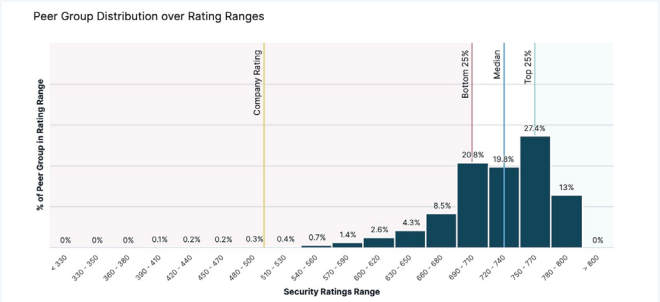
Security Rating

Provides an objective measure of security performance that informs trends over time.



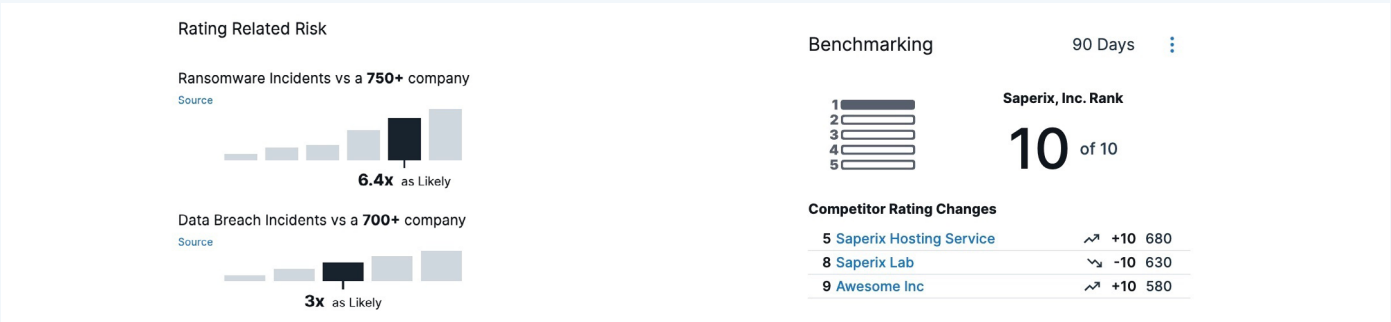
Peer Analytics

Provides context by comparing performance against industry peer groups.



Security Metrics

Provides context for meaningful discussions leveraging Key Performance Indicators (KPIs). Examples include likelihood of ransomware and data breach.



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