

Bitsight Security Ratings Correlate to Breaches

The only security ratings platform that indicates the risk of a publicly disclosed data breach.

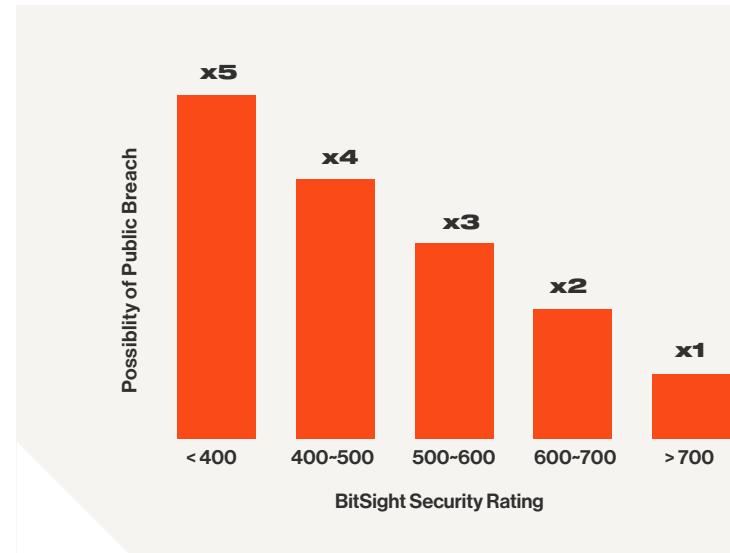
Background

Bitsight Security Ratings are used by organizations worldwide to mitigate cybersecurity risk across the enterprise. Leading organizations including AIG, Fannie Mae and Comcast depend on Bitsight to provide quantitative insight into the risks facing both themselves and third parties. As data breaches continue to grab headlines and create significant business challenges, more and more companies are actively seeking measurements for risk of a breach. By comparing its ratings to a comprehensive set of publicly disclosed data breaches, Bitsight can confidently demonstrate that Bitsight Security Ratings are the only ratings platform proven to indicate the risk of a publicly disclosed breach.

Study Overview

Bitsight analyzed the Security Ratings of 27,458 companies over a two year period. These companies varied by size and geography and they spanned 22 diverse industry sectors. Bitsight's data scientists compared this ratings data to a comprehensive set of 2,671 breach events during this time period. The resulting analysis demonstrates that companies with higher ratings are less likely to have experienced a publicly disclosed data breach.

Specifically, companies with a rating of 400 or lower were five times more likely to experience a publicly disclosed data breach than companies with a 700 or higher.



More than **27,000** Companies examined in this study



Nearly **3,000** Breaches observed from companies of various sizes and industries



Companies with a **high rating** are **less likely to experience** a publicly disclosed breach

Business Impact

Organizations across all industry sectors can leverage this information to drive risk aware business decisions. Security Ratings are indicative of a company's risk of data breach, and businesses can take action with Bitsight Ratings in the following ways:

- ▶ **Continuously monitor the cyber security performance of third party vendors.** Prioritize which vendors need a follow up or onsite assessment. Communicate with vendors with low ratings to ensure that issues are being addressed. Empower vendors to lower their risk of a breach.
- ▶ **Benchmark the security performance of an organization.** Communicate to upper level management on what ratings mean and on the importance of historical data. Provide comparative analysis to benchmark data breach risk among industry peers. Remediate issues with detailed forensics to lower your risk of a breach.
- ▶ **Prioritize cyber insurance applicants.** Determine cyber insurance policies and coverage based on risk of a breach. Underwrite good risk. Continuously monitor your book of business to make sure that insureds do not increase their likelihood of a breach.
- ▶ **Monitor merger and acquisition targets** for security problems from discovery through due diligence and purchase. Communicate with portfolio companies and subsidiaries about cyber risk. Enable acquisitions to continuously manage cyber risk to prevent a potentially costly breach.

Notes

Bitsight worked with a data breach registry maintained by Advisen, a leading insurance consultancy firm.



Interested in learning more? Check out a copy of our slides that include this data and additional analysis. Ask your Bitsight representative for more information.

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

