CYBER RISK SCORE

The ISS Cyber Risk Score is a data-driven scoring and screening solution designed to enable objective assessment of the cyber risk posture of any company. The Cyber Risk Score represents the relative likelihood that an organization will suffer a material cyber incident (e.g., breach) within the next 12 months. Each company's Cyber Risk Score is generated from data findings collected from publicly accessible cyber assets identified as being either owned or operated by the subject company or any of the subject company's majority-owned subsidiaries. The attribution of cyber assets to a company (or its majority-owned subsidiaries) is reviewed at least annually, while each week a new score is generated based on findings collected over the previous week. Historical scores and data provide greater context and trend analysis to understand a company's approach to managing cyber risk over time.

Outputs

The Cyber Risk Score is calculated using variables based on the subject company's network and domains, and on the subject company's riskiest sub-organization networks. The overall cyber risk posture of a company is represented as a single, concise score on a scale from 300 to 850. A score of 300 represents a high risk; a score of 850 represents a low risk. A company with a Cyber Risk Score closer to 300 is at significantly higher risk of experiencing a material cyber incident in the next 12 months than a company with a Cyber Risk Score closer to 850.

The scoring model also calculates and returns each company's Firmographic Max. This is the maximum score that the company could attain, in the absence of any other measured cyber risk, given the industry in which they operate, as well as the size of the company, as measured by employee count. The Cyber Risk Score and the Firmographic Max are qualitative outputs.

The Cyber Risk Score model assesses organizational security posture across a wide range of indicators and provides a set of reason codes explaining the relevant properties associated with each. The reason codes should be viewed as general characteristics of present and historical security posture that can be applied to broad organizational activities rather than specific malicious activities.

Research Process

- Data collection: The Cyber Risk Score model produces a score based on a diverse dataset collected regularly by ISS. This dataset incorporates elements indicative of organizational security posture on endpoints, software services, and infrastructure configuration. The rate at which various data sources are refreshed in the Cyber Risk Score portal ranges from daily to weekly. All profiled companies are rescored weekly. Both qualitative and quantitative information is considered in the scoring process for the Cyber Risk Score.

- Quality assurance: Every company is scored using the same scoring model. ISS retrains and releases an updated scoring model on an annual basis. This allows the Cyber Risk Score analytics team to review and retest the predictive qualities of the data-finding features used in scoring as well as re-train the model on the latest known cyber breach data.

  The analytic model constituting the scoring engine of the Cyber Risk Score product is trained to recognize patterns and signatures indicative of cyber breach risk. A historical dataset with

known breach outcomes is used for model training. Records of cybersecurity breach incidents are continuously identified by ISS and used to identify affected organizations and the corresponding timeline of breach incidents.

- Data validation: The Cyber Asset Review process allows subject companies to review the listing of collected cyber-attributed assets which make-up the company's external footprint. While ISS takes great care in the development and adherence to the Cyber Risk Score cyber asset attribution methodology, misattributions can and do occur. ISS encourages all companies to review their own Cyber Risk Score and the cyber assets that have been attributed to them for scoring. Through this process, companies can identify any cyber assets that they believe should be added or removed from their company profile.

Every covered company is invited to log in, free of charge, to the Cyber Risk Score platform to review its attributed cyber assets for accuracy and completeness. Companies may submit any change requests directly within the platform and those change requests will then be reviewed by the ISS data team, according to the Cyber Risk Score cyber asset attribution methodology.

Use of Estimated Data

ISS Cyber Risk Score does not incorporate any estimated data as the inputs are based only on disclosed or collectable data.

Last Reviewed: January 2024

We empower investors and companies to build for long-term and sustainable growth by providing high-quality data, analytics, and insight.

SUCCEED WITH ISS ESG SOLUTIONS

Email sales@iss-esg.com or visit iss-esg.com for more information.