Determining the EJPS Cyber Risk Rating

Egan-Jones Cyber Risk Ratings Summary

Egan-Jones Cyber Risk Ratings helps companies assess their security posture (health) and address the critical areas for improvement in order to attain a strong score. Egan-Jones proxy analysts utilize Cyber Risk Ratings in evaluating a company's security and business risk, and to issue proxy vote recommendations.

EJPS analysts use the SecurityScorecard platform to ascertain the company's Score which is incorporated into the EJPS Proxy Research Report. The methodology utilized for determining the Score is outlined below.

Egan-Jones Cyber Risk Ratings Service

Cyber Risk Rating Methodology Summary
The Rating is based on tens of thousands of data points with assigned, weighted levels of severity that are analyzed by SecurityScorecard's proprietary platform and packaged into a score for every rated organization. Scores are expressed as A, B, C, D and F ratings. SecurityScorecard ratings are continuously updated and recalculated as new vulnerabilities are discovered, and when organizations improve their security.

Egan-Jones Cyber Risk Rating Quantitative Raw Score
Currently, the SecurityScorecard platform scores on 75+ issue types. These data sets are normalized, assigned weights, and aggregated into factor-level subtotals for a defined set of cohorts (based on industry and IP footprint). The factor level subtotals are then ranked, scaled and distributed over a numeric range of 50-99 (F-A). Factor scores are then combined on a weighted basis to produce the final total score.

Egan-Jones Cyber Risk Rating Qualitative Adjustment Factors
The scored factors include: Network Security, DNS Health, Patching Cadence, Endpoint Security, IP Reputation, Application Security, Cubit Score, Hacker Chatter, Information Leak and Social Engineering.

Qualitative Adjustments	Description
-	Network Security: Detecting insecure network settings
-	DNS Health: Detecting DNS insecure configurations and vulnerabilities
-	Patching Cadence: Out of date company assets which may contain vulnerabilities or risks
-	Endpoint Security: Measuring security level of employee workstations and mobile devices
-	IP Reputation: Detecting suspicious activity, such as malware or spam, within the company network
-	Application Security: Detecting common website application software vulnerabilities
-	Cubit Score: Proprietary algorithm checking for implementation of common security best practices
-	Hacker Chatter: Monitoring hacker sites for chatter about company
-	Information Leak: Potentially confidential company information which may have been inadvertently leaked
-	Social Engineering: Measuring employee awareness to a social engineering or phishing attack

The positive impact on a factor score for a specific entity can be re-calculated when a specific issue is resolved. This means that remedial action can mitigate the vulnerability and raise the score.

Specifically, during any calendar quarter, company scores may be adjusted positively when the following remedial steps occur:

- Upon notification from EJPS, a rated company contacts Egan-Jones / SecurityScorecard for the purpose of clarifying or performing remedial action in their infrastructure
- The rated company can access their company scorecard to obtain details about observed vulnerabilities
- SecurityScorecard will provide a consulting session to assist in remediation of the observed vulnerabilities
- After changes are made to close "Open Issues", SecurityScorecard will re-scan the company and adjust the score accordingly

Egan-Jones Openness and Transparency

In addition to the information published (at no cost) in this document and that is disclosed on our website, EJPS offers both volume and individual licensing to its intellectual property, reports, data and models, at fair and reasonable cost, to all interested parties. A model license is also included for clients who subscribe to our highest tiers of research service at no additional charge. Please contact sales@egan-jones.com for more information about licensing any EJPS intellectual property.