riskrecon

mastercard

RiskRecon Ratings Explained

The foundations, the ratings scale, and correlation to data breach event frequency

December 2020

RiskRecon.com

sales@riskrecon.com

Boston, MA

Salt Lake City, UT

(801) 758-0560

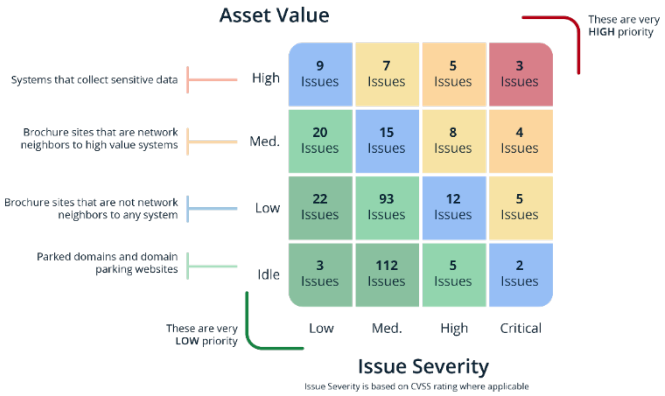
Introduction

The RiskRecon cybersecurity risk ratings platform enables professionals to confidently make risk decisions rapidly, providing ratings that assess real-world cybersecurity risk management quality. The ratings model founded on RiskRecon's unique ability to automatically risk prioritize issues based on issue severity and the value at risk of the system in which each issue exists. This yields a risk-responsive model that provides you useful ratings and actionable insights that pinpoint risk in your ecosystem.

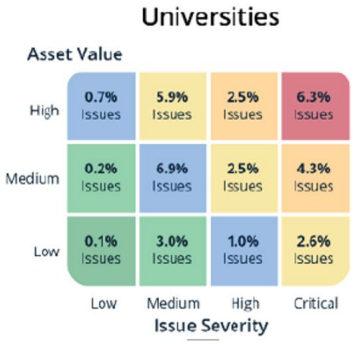
RiskRecon rates the quality of an organization's cybersecurity risk performance using an A – F labeled scale and 0.0 – 10 numeric scale. The rating is based on the rates and risk priority of issues present in the environment as observed by RiskRecon's passive risk assessment algorithms. This paper explains RiskRecon's A – F / 0.0 – 10 rating scale. A full explanation of RiskRecon's assessment and rating methodology is available for download at https://www.riskrecon.com/cybersecurity-risk-rating-model.

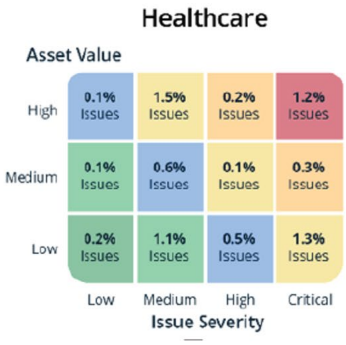
The Foundation

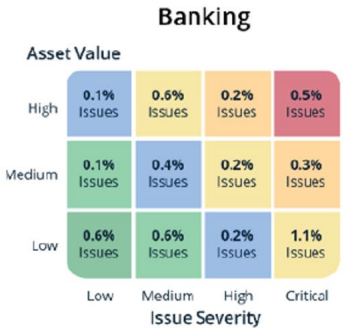
There are two key points to understand about RiskRecon's rating model. First, RiskRecon rates risk on the foundation of knowing the rates of issues in an environment based on the combination of issue severity and asset value. As such, critical severity issues in high value systems have the highest weight, whereas low severity issues in low value systems have the lowest weight. Issues in idle value assets (parked domains and domain parking websites) often have no weight in determining the rating.



Second, RiskRecon's ratings reflect the level of cybersecurity quality of an organization as observed in the reality of "known good" and "known poor" risk management performance. This was accomplished through industry-level analysis of the rates and risk priority of issues present in organizations. In doing so, RiskRecon discovered that large banks have the lowest rate of issues across all dimensions of risk priority, while universities have the highest. For example, large banks have 0.5 critical severity issues per 100 Internet-facing systems, whereas universities have 6.3 critical severity issues per 100 Internet-facing systems.





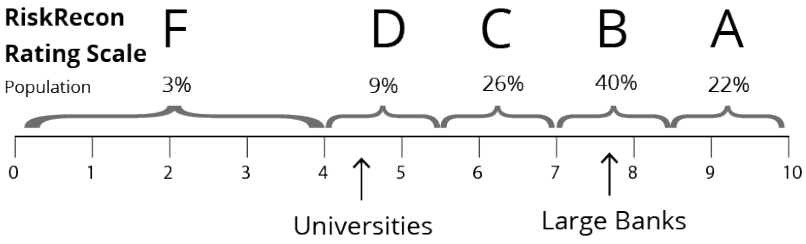


Based on this foundation of objectively observed "known good" and "known poor" risk management, RiskRecon built a rating model that intentionally anchored large banks at a rating of 7.8 and universities at a 4.5. To achieve this, RiskRecon discovered the weights to assign for each issue for every combination of severity and asset value. RiskRecon then determined the weights necessary to assign at the security criteria and the domain levels, into which the individual issues fold into.

While RiskRecon did not build a model to correlate with historical breach events, the rating model does strongly correlate with breach event rates.

The Rating Scale

RiskRecon rates cybersecurity risk management performance on a scale of 0.0 – 10, sub-dividing them into A – F ratings. The graphic below shows the rating scale and the population percentage of each rating tier across the entire RiskRecon population.

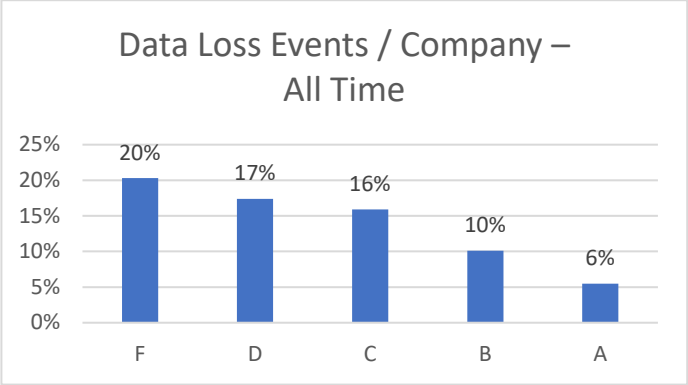


RiskRecon determined the math behind the model necessary to set the average rating of large banks ("known good") to a 7.8 and the average rating of large universities ("known poor"), using a Rayleigh 3 model to dis to 4.5 and using a Rayleigh RiskRecon then used a Rayleigh 3 statistical algorithm to distribute organization performance ratings across the spectrum. Performance analytics are largely founded on the rates of issues by asset value and severity to minimize bias based on organization size.

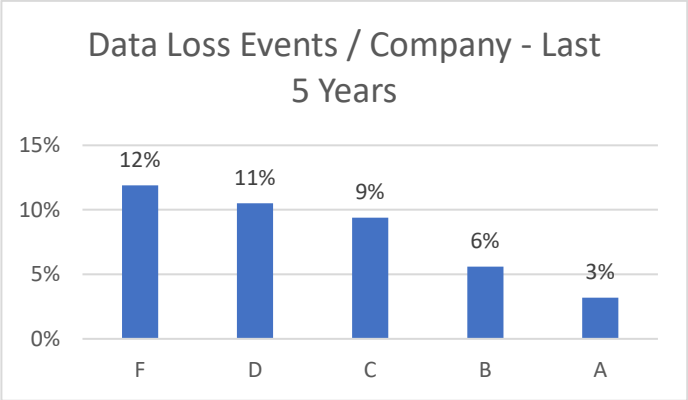
Rating	Range	Population	Description
A	8.5 - 10	22%	A-rated organizations perform within the top 22% of all assessed companies, presenting either no material issues of risk in their environment or presenting a very small rate of material issues and also a low rate less material issues. A-rated organizations present a stronger risk-prioritized issue profile than large banks. Companies that have a very small infrastructure often rate as an "A" or an "F" as the rate of issues in their environment is more Boolean. For example, their systems are either patched (100%) or not patched (0%). As such, an A rating for a very small company is informative only to the extent that RiskRecon did not identify any issues; however, it should not be relied to infer that they have robust risk management processes as achieving an A rating across such a small infrastructure does not require significant discipline. In comparison, it is more challenging for medium and large companies to achieve an "A" rating as they must perform well across a much wider range of systems.
B	7.0 - 8.4	40%	B-rated organizations perform within the top 42% to 78% of all assessed entities. In building the rating model, RiskRecon anchored the performance of the 100 largest global financial institutions at a 7.8. These organizations typically manifest a small rate of material issues in one or two security domains, in combination with a larger number of less material issues.
C	5.5 - 6.9	26%	C-rated organizations perform below average, being in the performance range of 13% to 38% all assessed entities. These organizations manifest a low rate of material issues in multiple security domains or have a high rate of material issues in one or two security domains.
D	4.0 - 5.4	9%	D-rated organizations are in the bottom 12% of all assessed entities. These organizations have a high rate of material issues in multiple security domains.
F	0.0 - 3.9	3%	F-rated organizations are in the bottom three percent of all assessed entities. These organizations have a high or very high rate of material issues in multiple security domains.

Rating Correlation to Breach Events

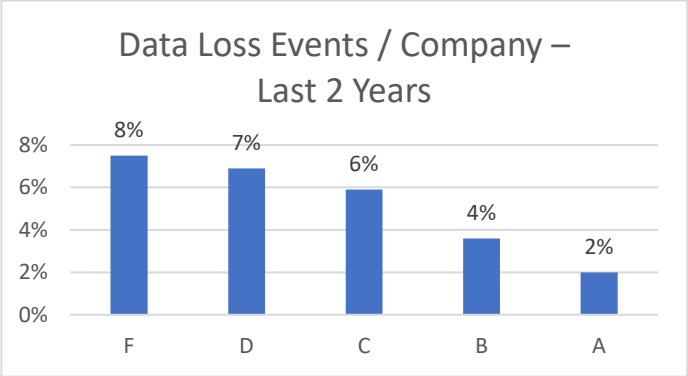
While RiskRecon did not build a model to correlate with historical breach events, the rating model does strongly correlate with breach event rates. Companies that perform in the upper tiers of the RiskRecon rating model have dramatically fewer breach events per company. For example, when looking at the entire history of data breach events, A-rated organizations have a 3.3x lower rate of breach events in comparison with F-rated organizations.



Data loss events per company – all data loss events in entire company history
- A rated 3.3x lower rate than F rated
- A rated 2.8x lower rate than D rated
- B rated 2x lower rate than F rated
- B rated 1.7x lower rate than D rated



Data loss events per company – only data loss events in last 5 years
- A rated 4x lower rate than F rated
- A rated 3.7x lower rate than D rated
- B rated 2x lower rate than F rated
- B rated 1.7x lower rate than D rated



Data loss events per company – only data loss events in last 2 years
- A rated 4x lower rate than F rated
- A rated 3.5x lower rate than D rated
- B rated 2x lower rate than F rated
- B rated 1.7x lower rate than D rated