riskrecon

mastercard

Introducing the updated RiskRecon

Cybersecurity Risk Rating Model

Release date October 2020

RiskRecon.com

sales@riskrecon.com

Boston, MA

Salt Lake City, UT

(801) 758-0560

Table of Contents

Abstract

RiskRecon is a leading provider of cybersecurity risk ratings. Organizations throughout the world use RiskRecon's ratings to better understand and act on their cybersecurity risk across a wide range of contexts and use cases. In October 2020, RiskRecon is releasing an update to its cybersecurity rating model. The model is founded on RiskRecon's unique ability to automatically assess cybersecurity risk performance based on the dimensions of the prevalence and severity of issues and the value at risk in the systems in which the issues exist.

This paper details RiskRecon's new rating model, explaining the rating math, the rating methodology, and the rating scale. To help frame the update, this paper provides insight into the performance rating distributions for several industries and some example third-party risk portfolios. A section is also dedicated to explaining updates to the RiskRecon user interface necessitated by the new rating model.

Introduction

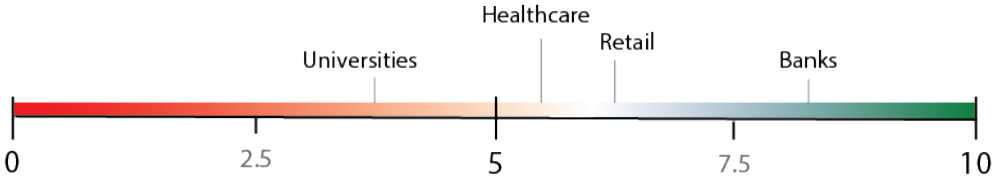
Enterprises operate in a complex digital ecosystem that interconnects with a wide range of customers, vendors, and partners through which data is shared and transactions are processed. Managed well, the ecosystem is a safe platform on which the organization achieves its objectives while protecting its assets, meeting its legal and regulatory obligations, and protecting its reputation.

Cybersecurity ratings provide essential insights into the health of digital ecosystems, enabling better understanding and action on the risks that organizations face. Third party risk teams use cybersecurity ratings to make better vendor selection decisions and to hold existing vendors accountable to managing cybersecurity risks well. M&A teams use ratings to assess acquisition targets for latent cybersecurity liabilities. Internal security analysts use them to gain a wholistic understanding of their internet risk surface and related exposures. And CISOs and boards use ratings to benchmark their cybersecurity performance against peers and competitors.

The RiskRecon cybersecurity ratings platform enables people to confidently make risk decisions rapidly, providing ratings that assess real-world cybersecurity risk management quality. It is 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.

The Foundation – Risk Reality

Is your cybersecurity risk management "good", like a bank? Or is it poor, like a university? RiskRecon's rating model is founded on observed real-world risk management practices, rather than being based on "expert opinion", or one that is intentionally engineered to map ratings to past data loss events. It is based on analysis of entire industries in which those widely accepted to excel at managing risk (Banks) reflect the upper end of the ratings scale, and industries widely known to be very weak at managing risk (Universities) reflect the lower end of the ratings scale.



RiskRecon can clearly differentiate between enterprises and industries that manage risk well and poorly because of RiskRecon's ability to not only determine the rate of issues and their severity within an environment, but also the value at risk for each system in which the issues exist. Of this unique capability, Jack Jones, Chairman of the FAIR Institute and co-founder of RiskLens stated:

> "Far too much energy in information security is wasted on resolving issues that don't matter. As the FAIR model promotes, effective risk management requires understanding the probable frequency and magnitude of loss; that depends on understanding asset value. I am really pleased to see RiskRecon bring the ability to automatically determine asset value to market." [1]

Assessing Risk

Managing risk requires knowing 1) the rate of issues and their severity and 2) the value at risk for each system in which the issues exist. While identification of security issues and related severity is common, automatic determination of a system's value at risk is not. RiskRecon analyzes both dimensions and folds them into the rating model.

Issues

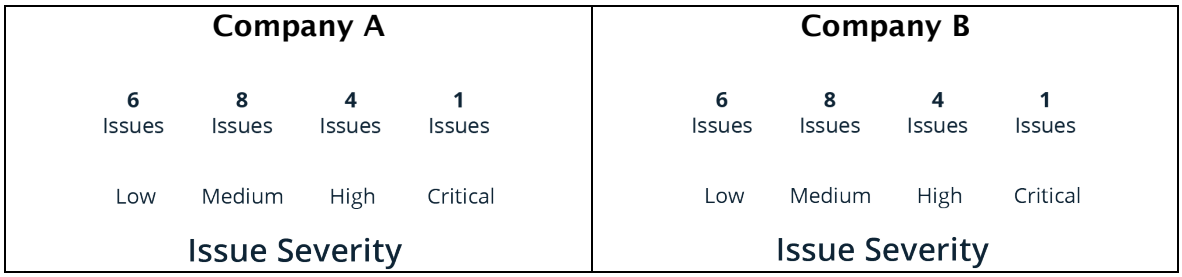
RiskRecon discovers issues present in an enterprises' Internet-facing systems and their operations through opensource intelligence and analytics. RiskRecon assigns each issue a severity rating of Critical, High, Medium, or Low using the Common Vulnerability Scoring System (CVSS). RiskRecon assigns its own severity rating for issues where a CVSS rating is not available.

Knowing the rate of issues and their severity in an environment provides visibility into how effective an enterprise is at managing issues. However, knowing the issues does not reveal how well it manages risk. Consider two different organizations that operate the exact same number

[1] https://www.prnewswire.com/news-releases/riskrecon-invents-ground-breaking-asset-risk-valuation-algorithms-transforming-how-enterprises-manage-third-party-cyber-risk-300730415.html

of systems, each system having the exact same data and functionality. Both environments have the same number of issues of the same severity, as shown in the graphic below.

Question: Which organization is better managing risk?



Answer: You cannot answer the question.

Why? Because you do not know the value at risk of the systems in which each issue exists. Do the issues exist in a brochure site that is rarely visited? Do the issues exist in a customer transaction portal where they are authenticating and submitting sensitive data? This kind of information is necessary for assessing risk. Enter RiskRecon's ability to automatically determine asset value.

Asset Value

RiskRecon automatically determines the value at risk of every system it analyzes. Combined with knowing the rate of issues and their severity within an enterprise, it enables RiskRecon to assess the quality of risk management.

Knowledge of the value at risk is essential to assessing risk. Without it, at best you can assess issues.

Question: There are two systems, each with the same issue – invalid HTTPS certificate subject. Which issue is higher risk?

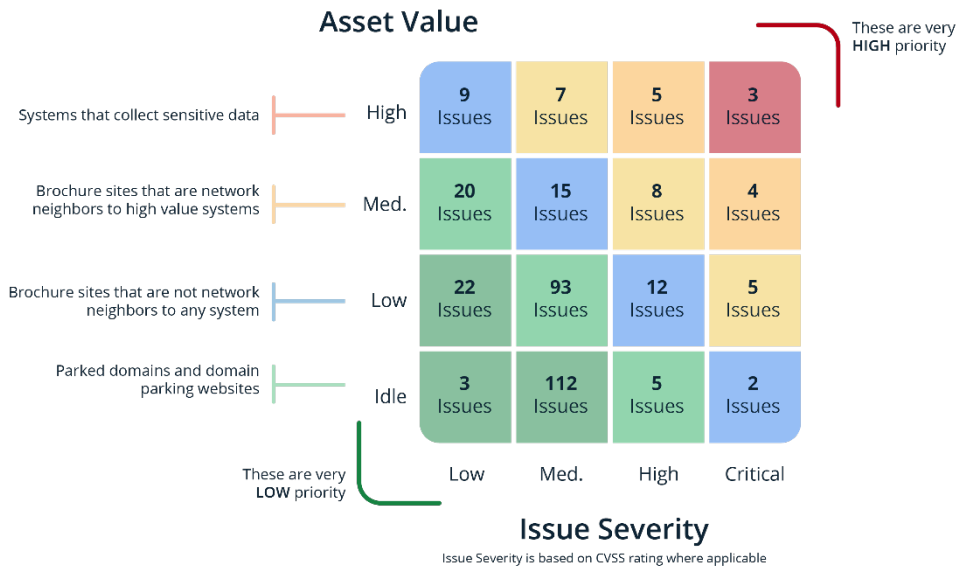
Answer: It is impossible to answer without additional information.

Let's add some more information.

Question: There exists a brochure site and a banking portal, each with the same issue – invalid HTTPS certificate subject. Which issue is higher risk?

Answer: Of course, the higher risk issue is in the banking portal.

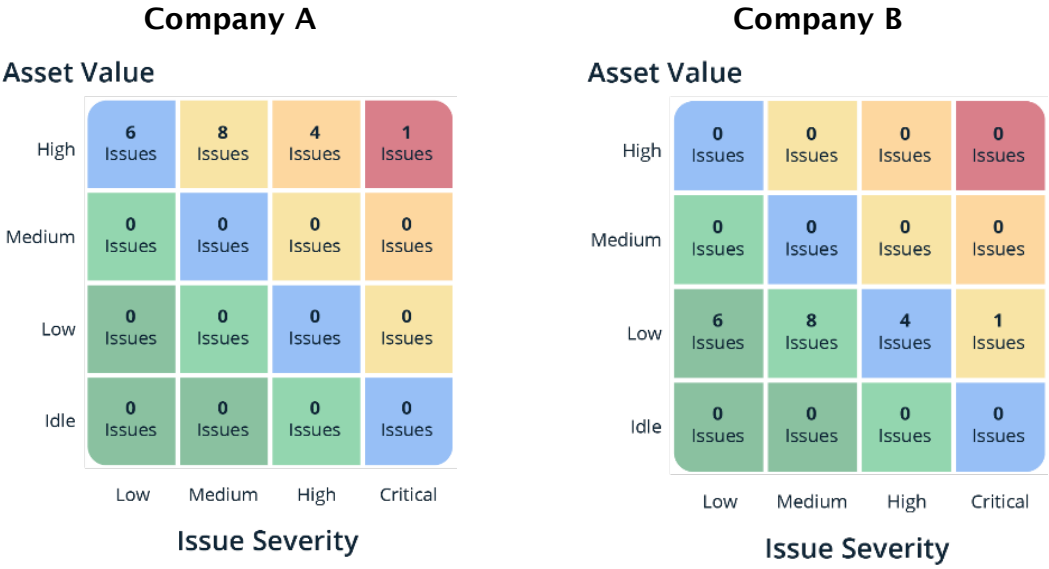
RiskRecon determines the value at risk (asset value) of a system based on deep analytics of the code, content, and configuration of each Internet-facing system. Through these analytics, RiskRecon discovers the types of data each system collects. The primary analytics are focused on identifying the form fields of every web page and using machine learning models to determine the types of data each collects. Systems that collect sensitive data such as user credentials, email addresses, credit card numbers, and so forth are rating as High asset value. Systems that collect no sensitive information are given a lower rating. RiskRecon uses other characteristics for determining asset value which are not described here.



Risk Prioritization

Combining issues and their severity with the asset value information we get a much more colorful picture through which we can assess risk. To illustrate this point, let's revisit Company A and Company B. Remember, they operate environments of the same size the provide the exact same functionality. They have the same security issues.

Again, the **Question:** Which organization is better managing risk?



Answer: Company B manages risk better.

With only knowledge of the count and severity of issues it is impossible to tell which better manages risk. However, adding the dimension of asset value changes the entire game. The issues of Company A all exist in systems that process sensitive data. In comparison, Company B only has issues in low value brochure systems.

The Rating Model

RiskRecon rates the quality of enterprise cybersecurity risk performance based on continuous collection and analytics of opensource intelligence signals that determine the rates and severities of cybersecurity issues within the context of the value at risk of the systems in which the issues exist. RiskRecon's risk assessment scope spans nine security domains built on approximately 40 criteria which assess systems against thousands of security tests.

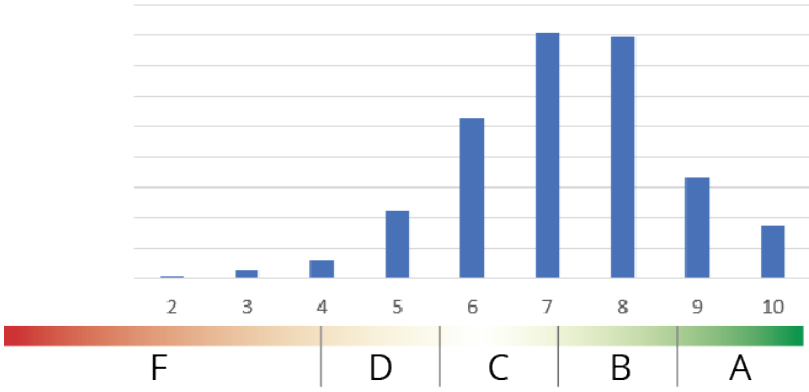
Rating Scale

RiskRecon rates cybersecurity risk performance on a scale of 0.0 – 10, with 10 being the best rating. RiskRecon overlays an A - F grading scale on top of the numeric ratings that separates performance into five bands. RiskRecon selected the five-tier grading system for two reasons. First, the A – F grading system is internationally familiar, with Wikipedia showing that at least 37 countries use the system for grading student performance. This aids consumers of the ratings in quickly understanding their own performance in relation to other companies. Second, five tiers provide useful portfolio-level performance segmentation, making it easier for analysts to identify and act on portfolio risk hot spots.

Grade	Rating Range
A	8.5 – 10
B	7.0 – 8.4
C	5.5 – 6.9
D	4.0 – 5.4
F	0.0 – 3.9

Ratings Distribution

Across the 46,000 companies monitored by RiskRecon the average rating is 7.3 – a solid B. RiskRecon intentionally set the rating ranges for each tier to force a planned distribution of companies to aid in ranking company performance and setting assessment priorities.



Portfolio-Specific Rating Distributions

The distribution of company risk performance varies based on the population of the portfolio being analyzed. The table below shows the rating distributions for two actual RiskRecon customer portfolios along with an example RiskRecon portfolio containing 46,000 companies.

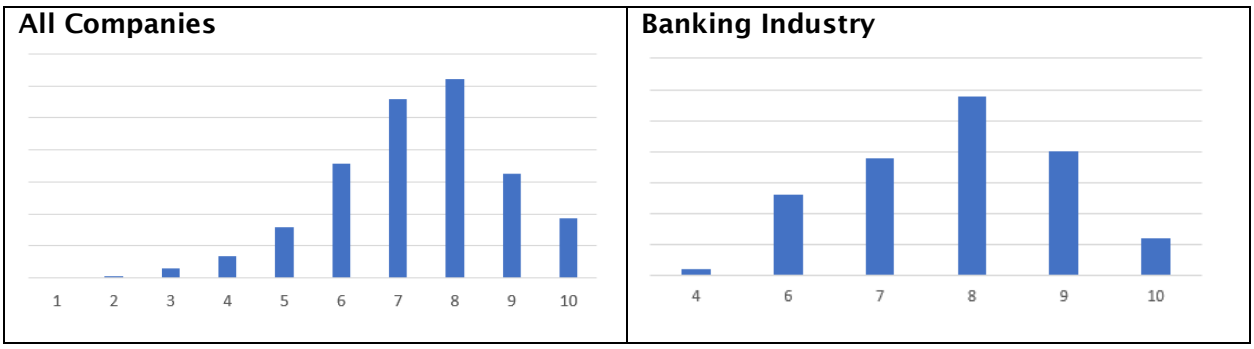
	RiskRecon Modeling Portfolio (46,000)	Credit Rating Company Vendor Portfolio (1,100)	Pharmaceutical Company Vendor Portfolio (5,200)
A	22%	18%	12%
B	40%	41%	38%
C	26%	31%	33%
D	9%	8%	12%
F	3%	2%	5%

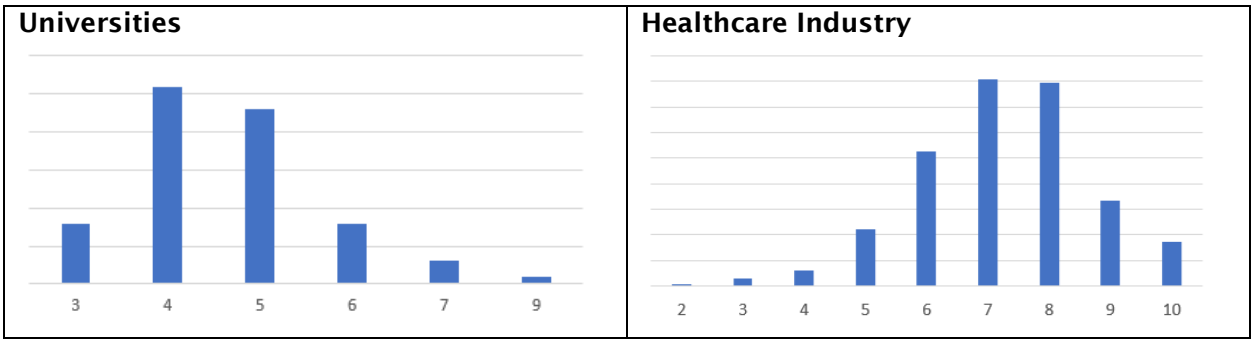
Industry Rating Distributions

Segmenting portfolios by industry reveals starkly different cybersecurity risk performance ratings and distributions. The banking industry has an industry average of 7.8 (a solid "B") with a very narrow variance, having almost no companies rating below a "C". In comparison, the healthcare industry has an average rating of a 7.2 with a much wider variance. Universities take up the tail end with a very low average rating of 4.5 ("D") with almost no organizations performing above a "C".

Rating Tier	All Companies	Banking	Universities	Healthcare
A	22%	30%	0%	17%
B	40%	45%	1%	41%
C	26%	25%	16%	31%
D	9%	0%	57%	9%
F	3%	1%	26%	2%
Avg. Rating	**7.3**	**7.8**	**4.5**	**7.2**
Variation	**2.4**	**1.3**	**1.7**	**2.0**

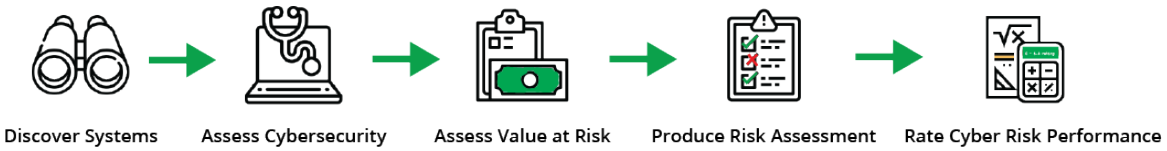
The graphs below visualize the ratings distribution for three industries.





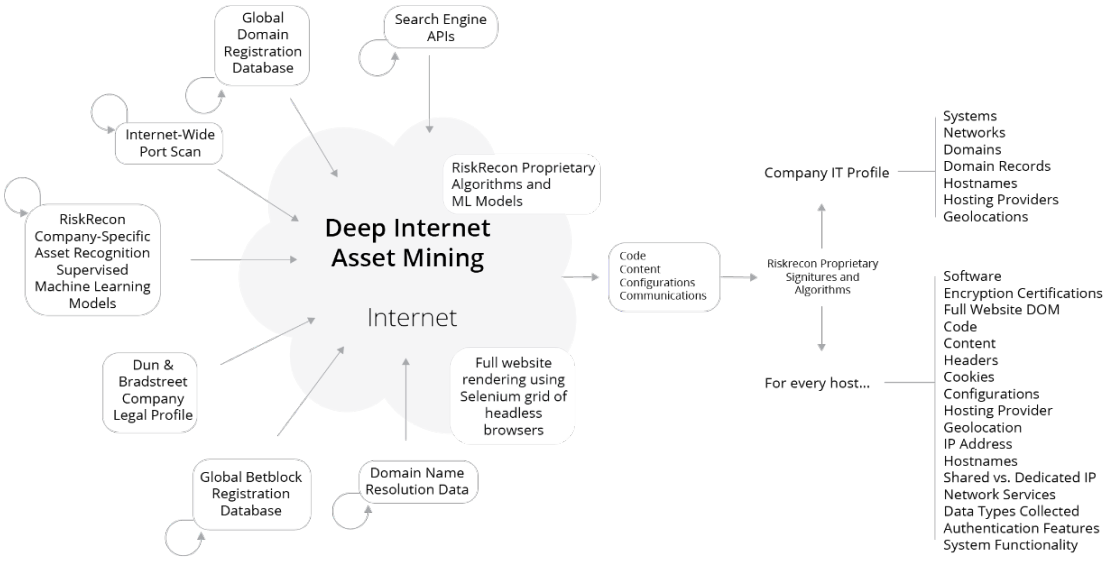
The Methodology

RiskRecon continuously monitors the cybersecurity risk performance of enterprises through open-source intelligence assessment techniques. All system discovery and security analytics are passive, based on collection and analytics of publicly available data. Through this approach, RiskRecon continuously monitors the cybersecurity risk of tens of thousands of companies. RiskRecon ensures accuracy of its assessment by operating its own system discovery through proprietary processes and algorithms. RiskRecon collects most of its security signals through direct observation, not relying on providers for which RiskRecon cannot optimize accuracy and scale. RiskRecon's accuracy in correctly attributing system ownership is independently certified to 98.5% accurate.



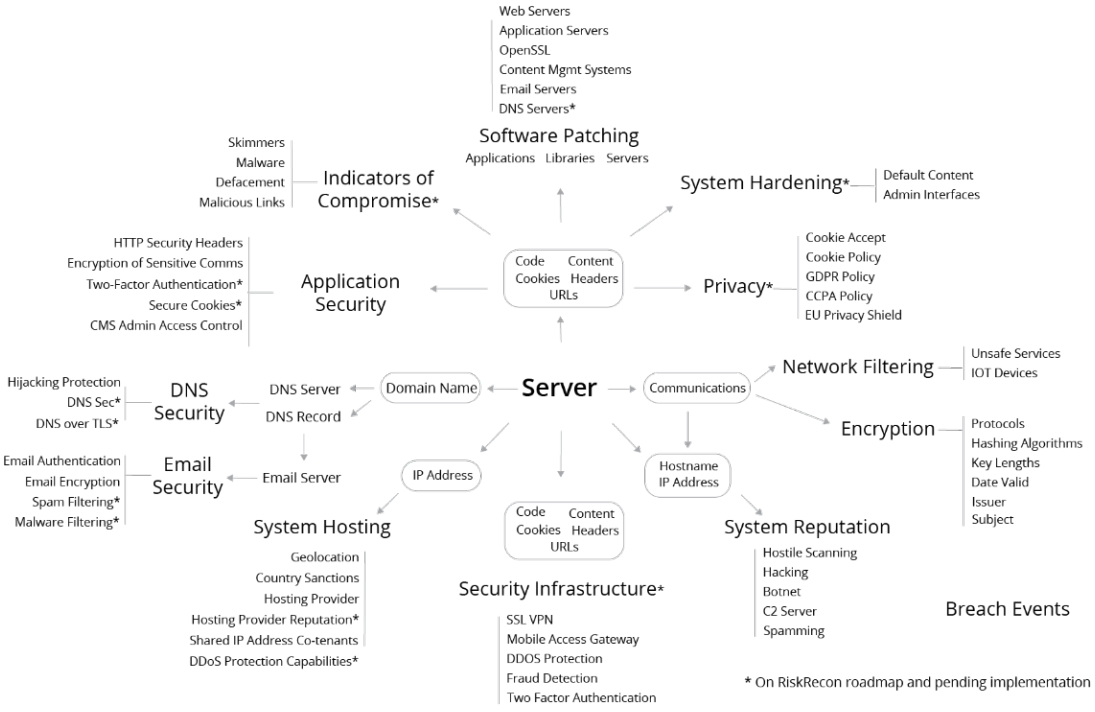
Discover Systems

RiskRecon maintains a continuous inventory of the enterprise internet surface, discovering systems using supervised machine learning algorithms that mine enterprise systems from the internet through examination of data collected from analysis of global domain and netblock registration databases, internet crawling, and subsidiary analytics. RiskRecon system ownership attribution is independently certified at 98.5% accuracy.



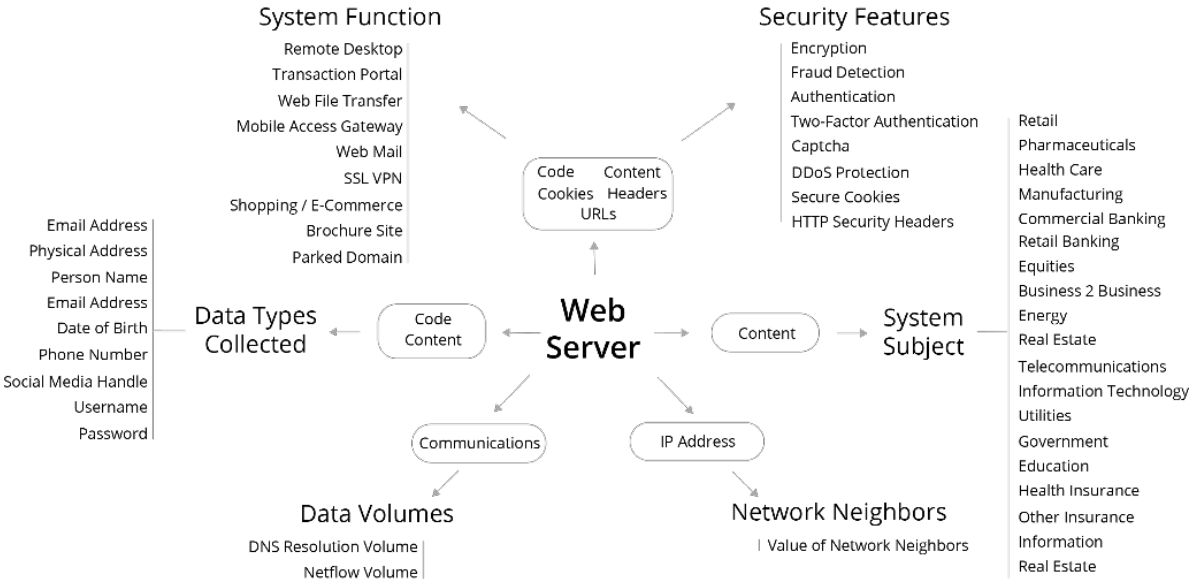
Assess Cybersecurity

RiskRecon continuously assesses cybersecurity performance using non-invasive techniques across nine security domains built on approximately 40 criteria that assess systems against thousands of security checks and monitors the larger enterprise for malicious activity and breach events. RiskRecon assesses performance to most criteria through direct observation using its own data collection and analytics, enabling strong control of assessment scope and accuracy. RiskRecon engages highly reputable providers for malicious activity and unsafe network services signals.



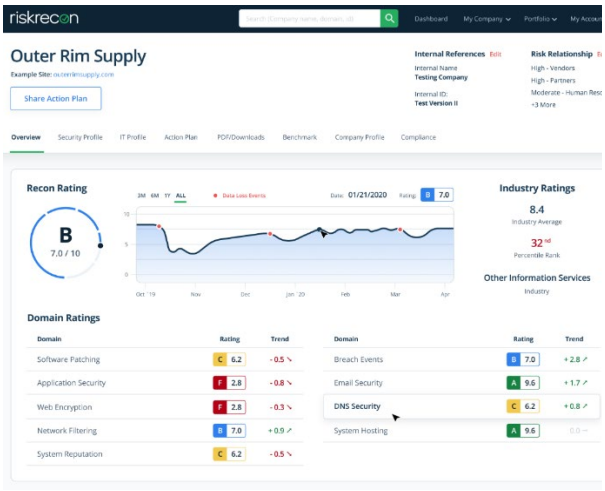
Assess Value at Risk

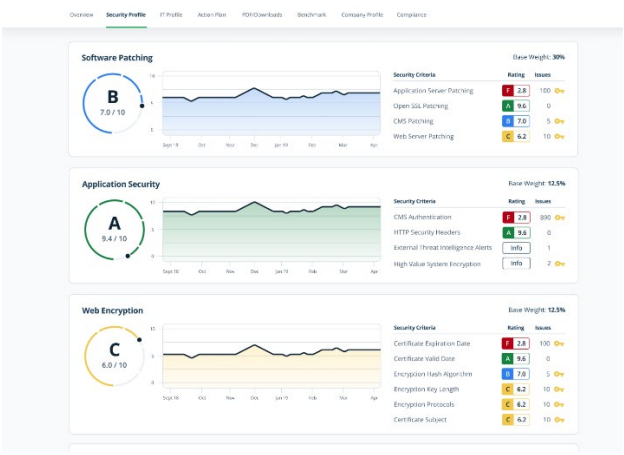
Determining the value at risk of a system is essential to assessing risk. Without it, one is limited to assessing systems for the presence of issues, but not risk. Assessing risk requires knowing the value at risk should a security breach occur. RiskRecon automatically and continuously determines the value at risk of each system through machine learning analytics of system code, content, and configurations. For example, RiskRecon can identify systems that require user authentication or that collect other senstive data such as names, email addresses, and credit card numbers. Similarly, RiskRecon can identify systems that are simply domain parking websites and brochure sites.

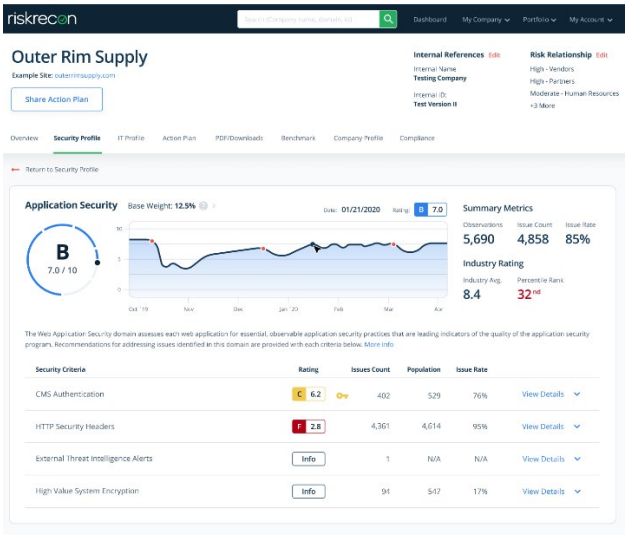


Produce Risk Assessment

Combining and analyzing the data collected through the system discovery, security assessment, and value at risk analytics, RiskRecon produces a robust risk assessment. RiskRecon assessments contain summary insights that highlight areas of strength and the key areas of weakness and related issues that expose the organization to the greatest risk. The assessments provide full details of the IT profile, the security issues, and related risk context and risk priority. RiskRecon maps assessment results to 12 industry security standards, enabling automated compliance assessment.





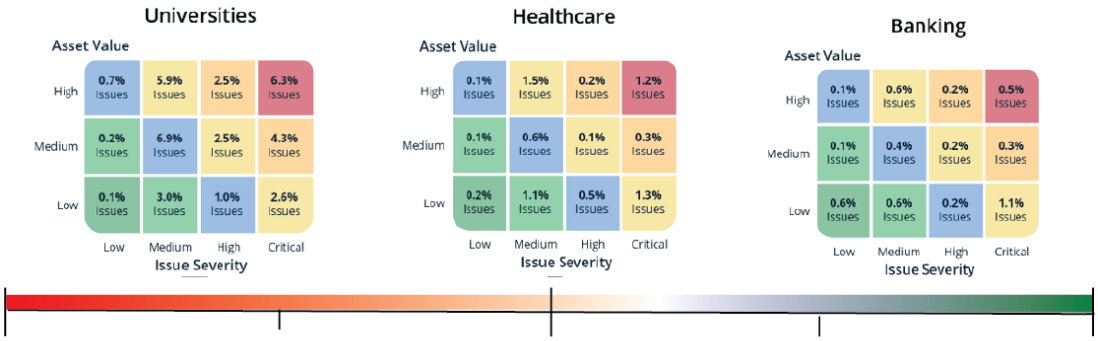


Rate Cybersecurity Risk Performance

RiskRecon assigns a cybersecurity risk rating for each enterprise, rating the quality of their overall performance. In addition to the overall rating, RiskRecon rates performance at the security domain and criteria levels. As explained earlier, RiskRecon's rating algorithm rates performance based on real-world cybersecurity risk management – is the enterprise managing risk well, like a bank? Or it is managing risk poorly, like a university. RiskRecon is uniquely positioned to rate cybersecurity risk performance within such real world context because only RiskRecon has the hi-fidelity risk insight based on the dimensions of the rates and severities of issues within the context of the value at risk in the systems in which the issues exist.

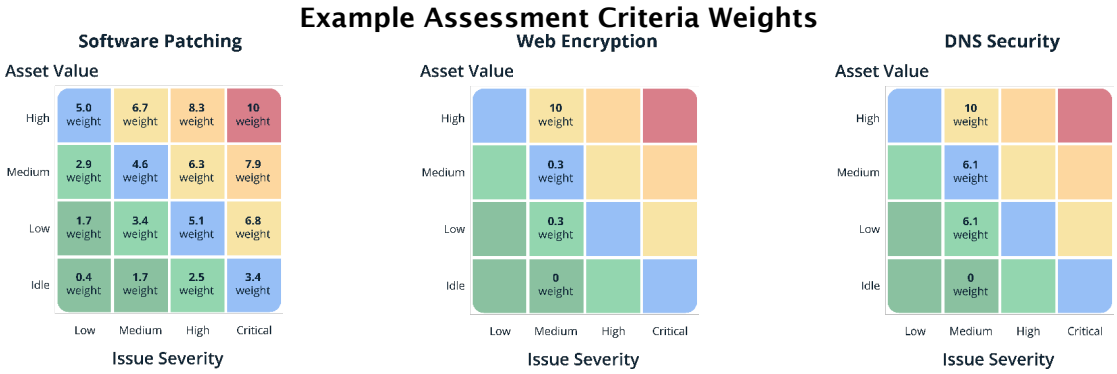
Banks vs Universities

RiskRecon's open source data plainly reveals that the banking industry manages risk well and universities manage risk quite poorly. When analyzing rates of issues within the context of issue severity and asset value, the banking sector stands above all others. As shown in the diagram below, banks have only 0.5 critical severity issues for every 100 high value systems (systems that process sensitive data). In comparison, universities have 6.3 critical severity issues for every 100 high value systems that they operate on the internet.



Criteria Issue Rating Weights

Leveraging its high fidelity risk signals, RiskRecon built a rating model that mathematically represents the risk priorities of the banking industry as the benchmark of "good" risk management performance and spread the ratings across the scale using universities as the benchmark of "poor" risk management. RiskRecon used the Rayleigh 3 statistical algorithm to ensure the weights distributed performance of all companies properly above bank ratings (they are good, but they are not perfect), below universities (yes, some are worse!), and in between. Some weighting schemes for some of the criteria are shown below.



Notice that there is a weight for every issue across each security criteria for every combination of issue severity AND asset value. That is a lot of math! Why Is that important? Well, consider again the example given earlier regarding web encryption. Where is proper use of web encryption most important? In systems that collect or transit sensitive data. Where is it much less important? In systems that are brochure sites. As it turns out, the banking industry agrees. They put a very high-risk priority on proper encryption configuration for high value systems but place a very low risk priority on encrypting read-only brochure sites. In fact, banks care 33x more about proper encryption of high value systems communications than for brochure sites.

Calculating the Overall Rating

RiskRecon calculates the performance rating for each assessment criteria using the criteria issue weights described above. RiskRecon then combines the criteria ratings to calculate the domain ratings, and then combines the security domain ratings to calculate the overall rating. As was done for determining issue weights, RiskRecon determined weights for security criteria and domains based on the combinations that mapped to banks rating well and universities rating poorly.

To calculate the security domain and overall ratings, RiskRecon uses a weighted geometric mean, rather than an arithmetic mean. The benefit of using a geometric mean is that poor performance in one security domain, such as email security, it not overly diluted by strong performance in other domains. The further a criteria or domain rating drops below that of other members of the population, the greater the weight it has on the overall calculation.

The starting weights employed to calculate domain ratings and the overall ratings are shown in the table below. It is important to remember that these are "base" weights, but not the actual weights because the use of geometric weighted mean can dynamically increase or decrease the weight of a given criteria or domain from the base starting point.

Security Domain	Security Criteria	Weight in Calculating Domain Rating	Weight in Calculating Overall Rating
Software Patching	Application Servers OpenSSL CMS Web Servers Email Servers DNS Servers	100%	**30%**
Application Security	CMS Admin Authentication	50%	**12.5%**
	HTTP Security Headers	50%	
	Unencrypted Sensitive Communications	INFO (will move to rated in Q4 2020)	
	Links to Malicious Sites	INFO	
Web Encryption	Certificate Expiration Certificate Valid Date Hash Algorithm Key Length Encryption Protocols Certificate Subject	100%	**12.5%**
System Reputation	C2 Servers Botnet Hosts Hostile-Hosts: Hacking Hostile-Hosts: Scanning Phishing Sites Other Blacklisted Hosts Spamming Hosts	See separate explanation	**7.5%**
Breach Events		See separate explanation	**10%**
System Hosting	Shared IP Hosting	50%	**5%**
	Hosting Fragmentation	50%	
	Hosting Countries	INFO	
	Hosting Providers	INFO	
	Hosting Domain Surface	INFO	
	Hostname Surface	INFO	
Email Security	Email Authentication (SPF/DKIM)	50%	**6.25%**
	Email Encryption	50%	
DNS Security	Domain Hijacking Protection	100%	**6.25%**
	DNS Hosting	INFO	
Network Filtering	Unsafe Network Services	See separate explanation	**10%**
	IOT Devices		

The User Interface Updates

While RiskRecon continues to numerically rate cybersecurity risk performance on a scale of 0.0 – 10, RiskRecon is overlaying the ratings with a five-tier A – F rating scheme. This necessitates updates to the portal user interface and PDF reports.

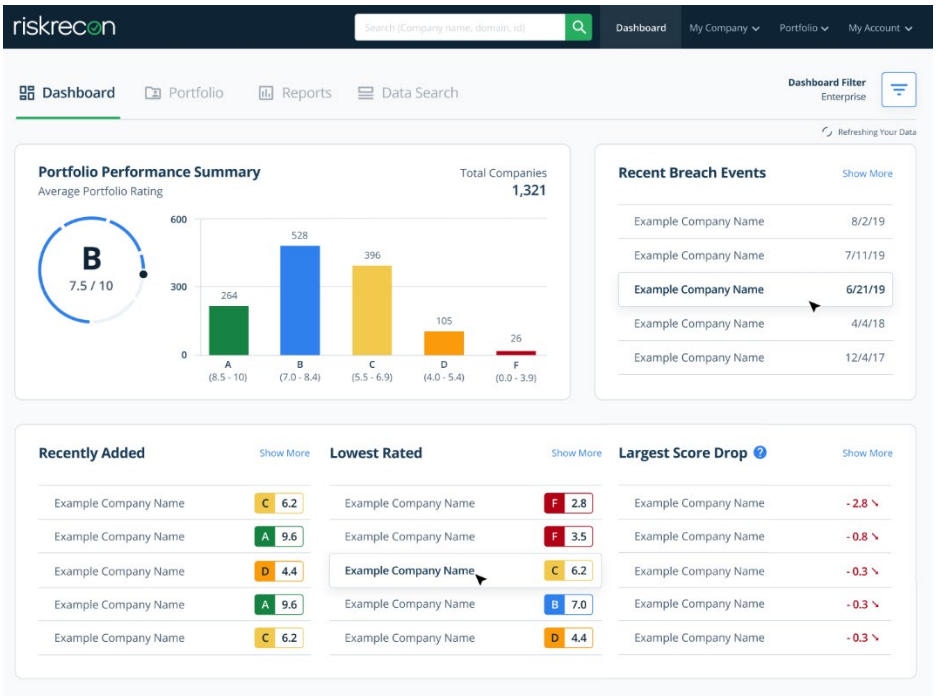
Core Elements

The iconography for large representation of ratings.

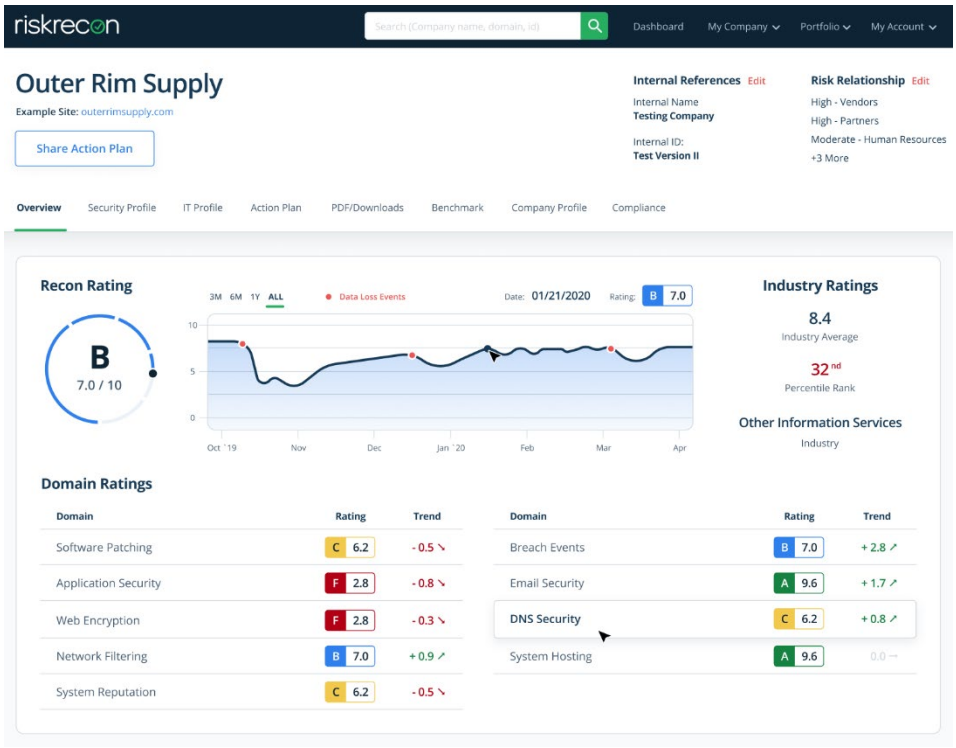
The iconography for compact representation of ratings.

Examples

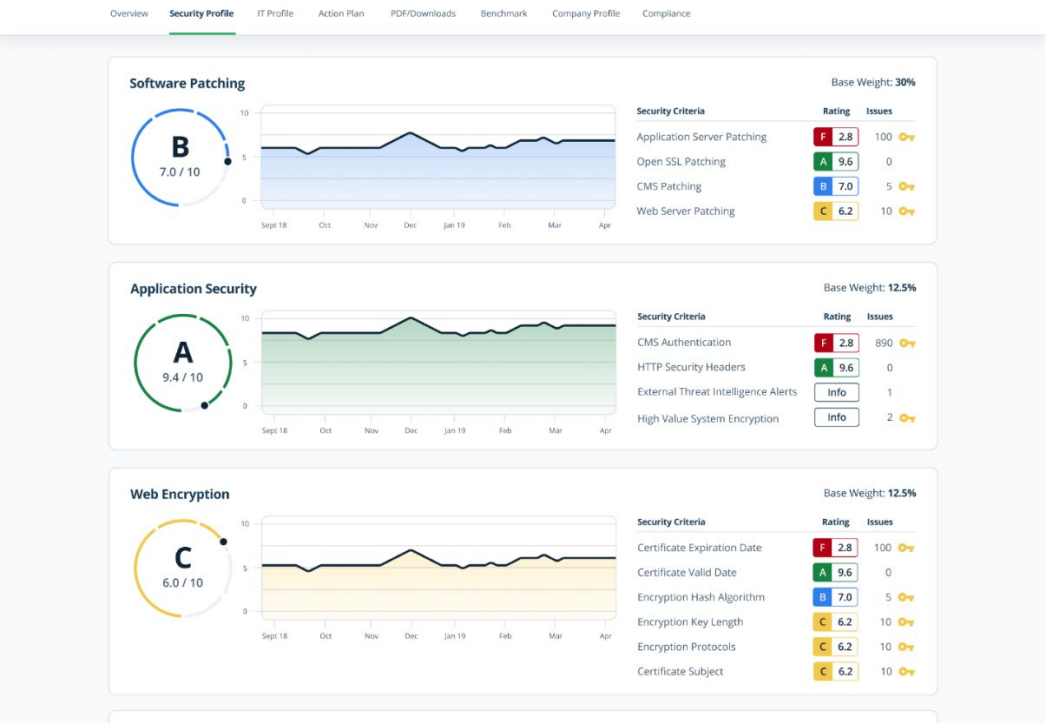
Portal Dashboard



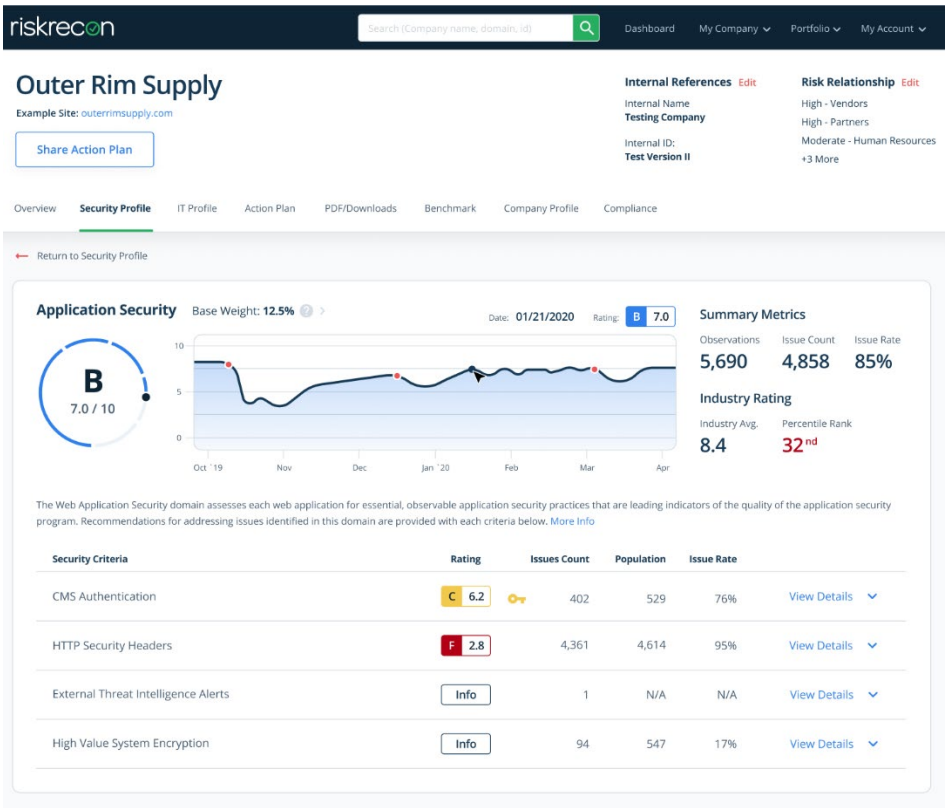
Company Overview



Security Profile Summary



Security Profile Detail



Conclusion

RiskRecon releases the new rating model in October 2020. In advance of the release, RiskRecon is working closely with customers to smoothly transition them to the new model.

RiskRecon produces cybersecurity risk ratings that enterprises can rely on to make better risk decisions faster. The new rating model produces ratings that reflect real world cybersecurity risk management. It is simple – based on outside passive assessment, does the organization perform like a bank or better, indicating strong performance? Or does the organization rate more like a university, having very poor performance? RiskRecon ratings reveal the answer.

RiskRecon's ratings are backed by continuous assessments of performance to tens of security criteria and thousands of underlying security checks. RiskRecon's assessments are true risk-based assessments, with every issue risk prioritized based on issue severity and asset value. No other platform does this automatically and at the scale of RiskRecon.

