RISKRECON

RiskRecon Cybersecurity Rating Model

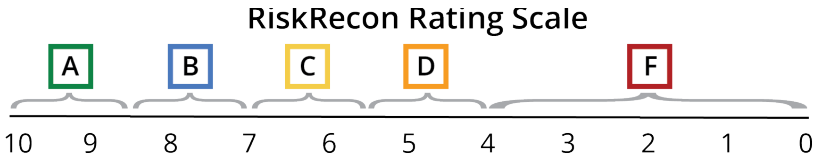
FEBRUARY 2024

RiskRecon makes it easier for you to understand and act on your cybersecurity risks across your entire supply chain. Central to that commitment is providing ratings that are aligned with risk management quality observed in the real world and that are strongly correlated to risk outcomes, such as destructive ransomware and data breach events.

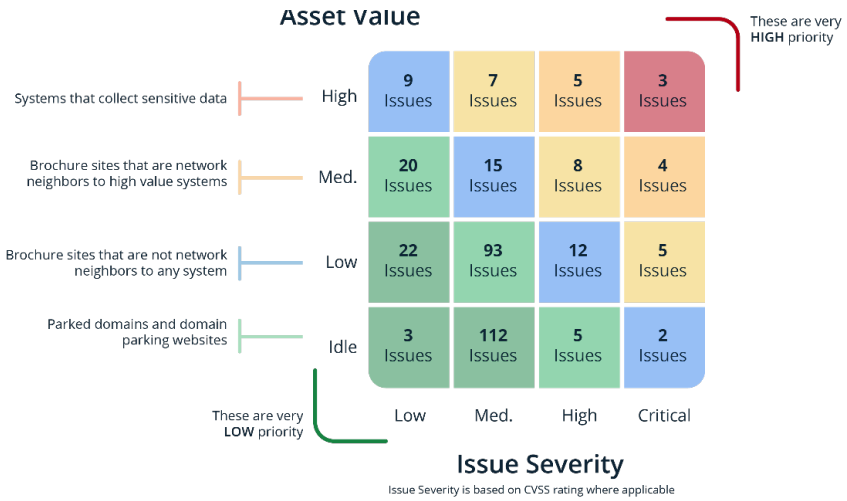
This is the third material iteration of RiskRecon's rating model, with the first accompanying RiskRecon's launch in 2015. The second was released in early 2020. This iteration, released in February of 2024, remains rooted in RiskRecon's unique ability to assess cybersecurity hygiene based on the prevalence and severity of a wide range of security issues within the context of the value of the assets within which the issues exist.

The Rating Scale

RiskRecon's rating scale remains the same as the previous iteration, which is an A-F scale, with the numeric rating ranges remaining the same.



The rating model continues to factor in the risk priority of issues based on issue severity and asset value. Issue severity is primarily aligned with CVSS rating. Asset value is based on the types of data and transaction capabilities of the system, in addition to the asset's proximity to assets of higher value. This provides better visibility into risk hygiene than just issue severity.



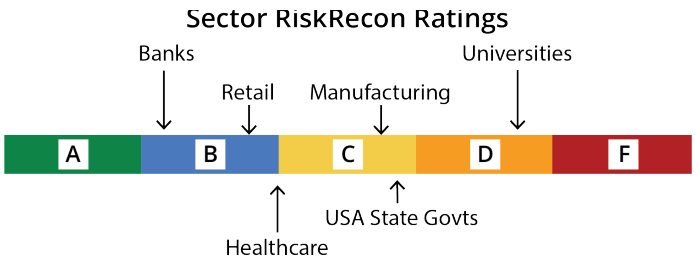
The Objective

The rating model is designed to achieve two objectives: be reflective of good cybersecurity hygiene as it manifests in the real world and to be strongly correlated with risk outcomes, such as destructive ransomware and the frequency of breach events.

<u>Reflection of the Real World</u>

Is the cybersecurity hygiene of that organization you are considering engaging to process your sensitive data strong, like a bank? Or is it weak, being more like a university's? RiskRecon's rating model is designed to reflect risk management practices observed in the real world, based on analysis of a wide range of industry sectors. As a sector, banks objectively manifest the best cybersecurity hygiene and higher education the poorest. The cybersecurity characteristics of these sectors, their rates and severities of vulnerabilities and types of vulnerabilities within the context of the inherent risk value of

the systems in which they exist inform the underlying mathematics and weights of the model. In lay person terms, banks have very few important issues in systems that process sensitive data and transactions, whereas universities have surprisingly large numbers of material issues in sensitive systems.



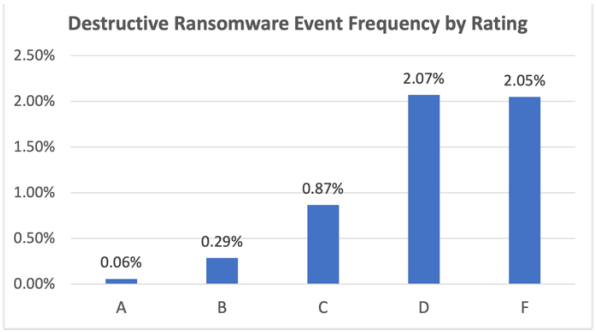
Correlated with Risk Outcomes

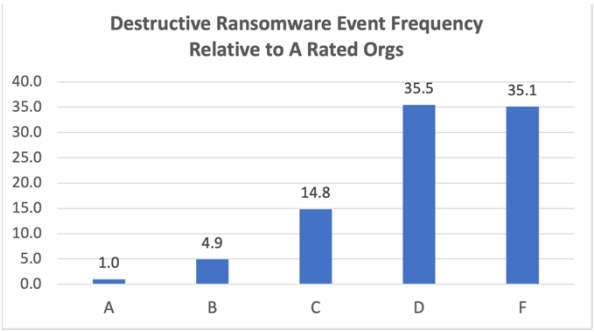
The rating model is also informed by the cybersecurity conditions of victims of destructive ransomware and data breaches around the time of the events to guide weights of different frequencies, types, severities, and contexts of vulnerabilities and conditions.

Destructive Ransomware

RiskRecon analyzed the cybersecurity hygiene conditions of 817 victims of destructive ransomware victims surrounding the time of the ransomware occurrence. The updated model has a very strong correlation with destructive ransomware events. Destructive ransomware events are those in which the victim's ability to operate is materially harmed due to encryption of one or more critical systems.

The rating model, when applied to RiskRecon's population of 150,000 analyst-supervised monitored organizations, reveals that those with very poor cybersecurity hygiene, rated as D or F, have experienced a 35x higher frequency of breach events compared to A rated organizations, which RiskRecon observes as having very clean hygiene.

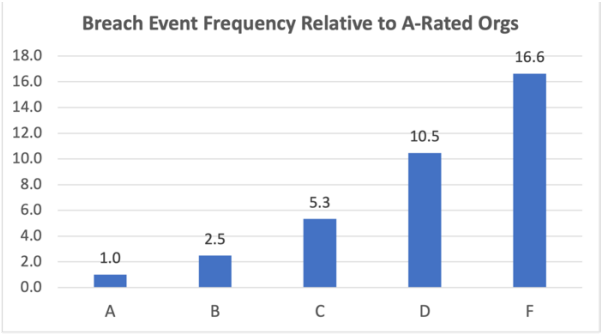


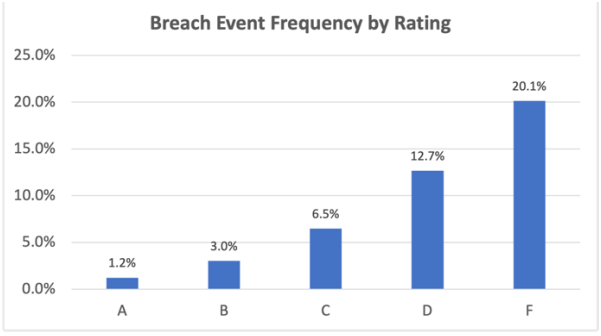


Breach Events

RiskRecon also informed weights of the rating model based on analysis of the cybersecurity hygiene conditions of companies related to 6,999 breach events. Breach events include all forms of ransomware and electronic data theft.

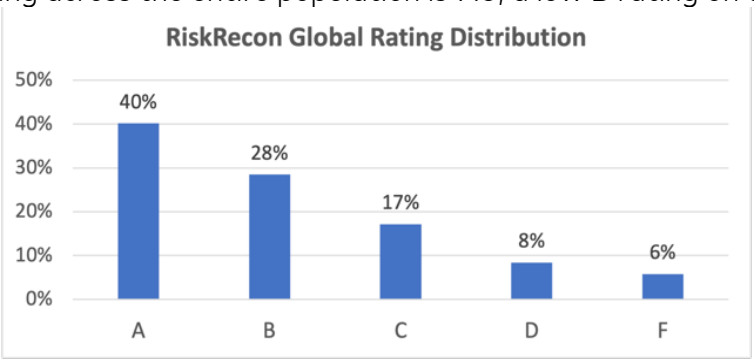
Those with poorest cybersecurity hygiene, rated F, have experienced a 16.6x higher frequency of breach events compared to A rated organizations, which RiskRecon observes as having very clean hygiene. In percentage terms, just over 20.1% of F-rated organizations and 12.7% of D-rated organizations have had at least one material breach event. In comparison, only 1.2% of A rated companies and 3% of B rated companies have publicly reported a breach.



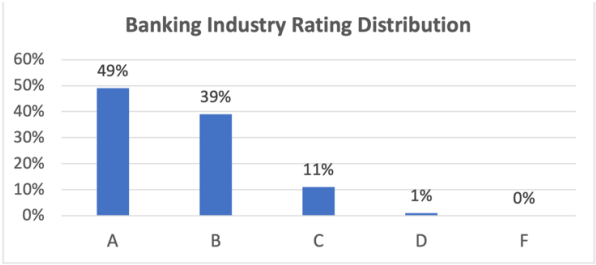


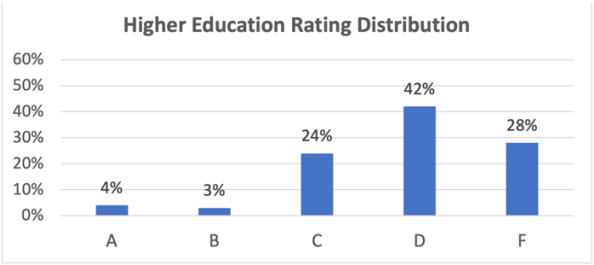
Ratings Distribution

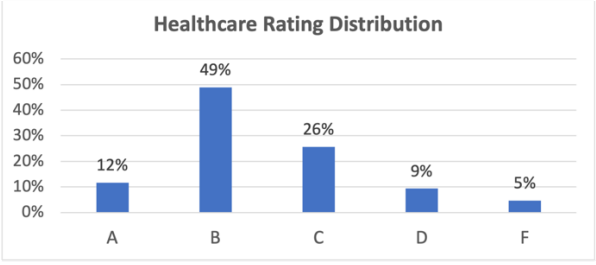
Across the 150,000 RiskRecon analyst-supervised company profiles, 14% of organizations are rated as D or F. The average rating across the entire population is 7.5, a low B rating on the A – F scale.

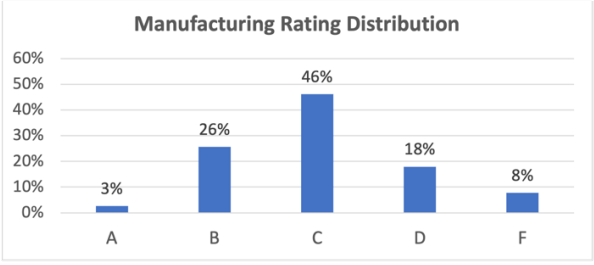


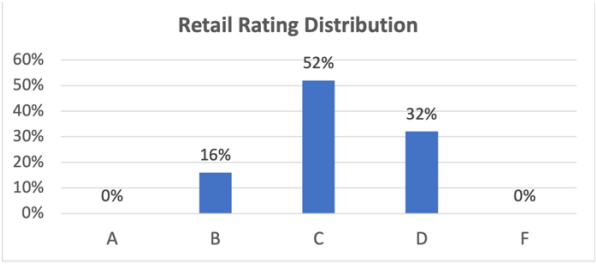
Looking at the ratings of the 50 largest organizations from six different industry sectors through the lens of this rating model reveals the stark contrast of cybersecurity quality between the sectors. In banking, 88% have an A or B rating and only 1% have a D or F rating. Higher education is nearly the inverse, with 70% rating a D or F and only 7% earning an A or B rating. Healthcare skews towards strong performing, where other sectors lean towards lower performing.

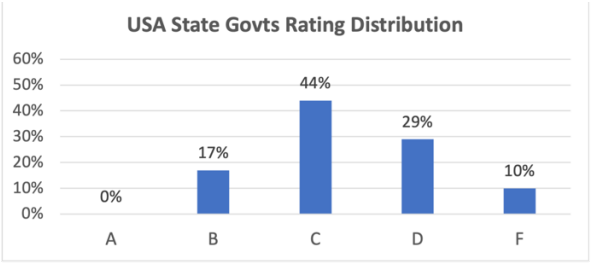










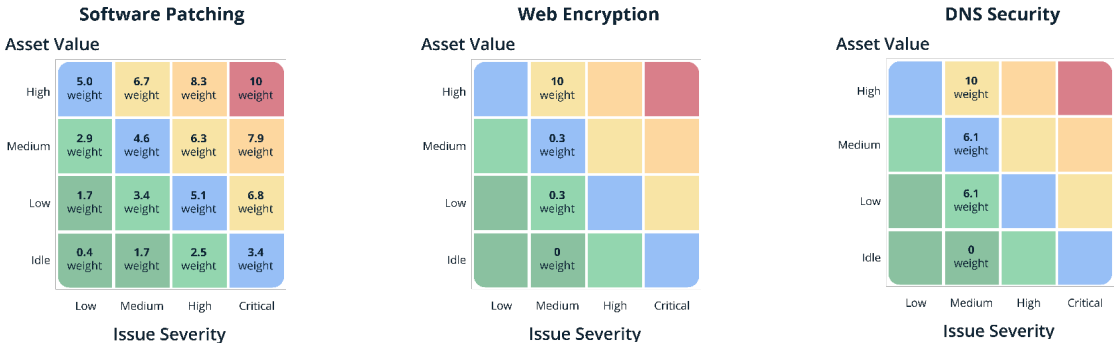


Rating Calculation

Step 1: Weighting Issues

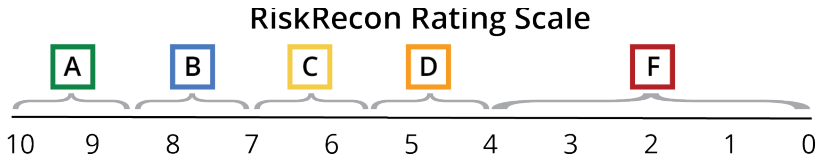
RiskRecon assigns a weight for each of the thousands of potential findings within the context of the finding criteria based on issue severity and asset value. The weighting is relative to the other combinations of issue severity and asset value for the given criteria. This differentiation of weighting a given finding based on asset value and issue severity is one of the remarkable differentiators of RiskRecon and why it can strongly correlate ratings to real world risk management and risk outcomes. For example, web encryption issues matter most in high value systems that collect and transit sensitive data and transactions, whereas it matters not in systems like domain parking sites, which RiskRecon automatically labels as idle.

Example Assessment Criteria Weights



Step 2: Calculating Domain Rating

The rating for each domain is calculated based on the frequencies of issues within the total system population, with findings weighted based on the value assigned based on asset value and issue severity for the given criteria. Each domain is rated on a numerical scale from 0 to 10, with 10 being the best. The numeric rating translates into an A – F rating scale, as shown below.



A geometric mean is used to calculate the domain rating for domains that consist of multiple criteria that are separately rated. Using a geometric mean, as opposed to a simple weighted average, results in criteria with ratings lower than the center having a greater effect on the domain rating the further they are from the weighted center. For example, assuming equal weights, if criteria A is 10, criteria B is 8, and criteria C is 2, then criteria C would take on a greater weight in determining the overall rating.

Note: The descriptions of the ratings of each domain and the underlying criteria are dramatically simplified, removing details of the specific mathematics and statistical models.

Software Patching - Domain Weight: 30%
The software patching domain rating is calculated based on the total number of software patching issues relative to the total population for each asset category, with each finding weighted based on issue severity and asset value.

Application Security – Domain Weight: 12.5%
The application security domain rating is calculated based on the weighted average of each criterion with the geometric mean applied in the final calculation. The rating for each criterion is calculated as follows:

- CMS Admin Interface Exposure – count of exposed admin interfaces relative to the total population of content management systems discovered. Weight 37.5%.
- HTTP Security Headers – count of systems missing any one of five HTTP security headers relative to the total population, factoring in the value of the asset in which the issue exists. Weight 37.5%.
- High Value Systems Encryption – count of high value systems that do not implement encryption relative to the total population of high value systems. Weight 25%.
- Malicious Code – if any malicious code is detected in any system, then the application security domain rating is set to zero, regardless of the ratings of other criteria. If no malicious code is detected, then the criteria have 0% weight. Weight 100% if any issue or 0% if no issue.
- External Threat Intelligence Alerts – info only.

Web Encryption – Domain Weight: 12.5%
The web encryption domain rating is calculated based on the number of HTTP encryption configuration issues relative to the total population of systems implementing HTTP encryption. The weight of each issue is determined based on issue severity and asset value. Encryption issues in high value systems that collect, and transit sensitive data have a very high weight relative to other systems, such as brochureware sites.

System Reputation – Domain Weight: 7.5%
The system reputation rating is calculated based on the weighted average of each criterion with the geometric mean applied in the final calculation, each finding weighted based on issue severity and asset value. The rating for each criterion is calculated as follows:

- C2 and Botnet Hosts – count of C2 and botnet hosts relative to the size of internet footprint. Weight 50%.
- Hostile Hosts: Hacking and Scanning – count of hosts exhibiting hostile activity relative to the size of the internet footprint. Weight 25%.
- Phishing Sites, Spamming Hosts, and other Exclusion-listed Hosts – count of hosts in these categories relative to the size of the internet footprint. Weight 25%.

Breach Events – Domain Weight: 10%
The breach events rating is calculated based on the number of publicly disclosed breach events, with each breach event impacting the rating for 15 months. The first breach event automatically reduces the rating to 4.5, which then increases linearly to 10 over 15 months. Additional breach events that occur while an existing breach event is impacting the rating further impacts the rating. Each breach event impacts the rating for 15 months.

System Hosting – Domain Weight: 5%
The system hosting rating is calculated based on the weighted average of each criterion with the geometric mean applied in the final calculation. The rating for each criterion is calculated as follows:

- Shared IP Hosting – the count of systems hosted at third-party hosting providers using shared IP addresses relative to the size of the internet footprint. Efforts are made to exclude content delivery networks and other infrastructure that requires shared IP addresses. Weight 50%.
- Hosting Fragmentation – the count of external hosting providers relative to the size of the internet footprint. The rating is based on deviation from the statistical norm for the given size category of the organization. Weight 50%.
- Hosting Geolocations – information only.

Email Security – Domain Weight: 6.25%
The email security domain rating is calculated based on the weighted average of each criterion with the geometric mean applied in the final calculation, each finding weighted based on issue severity and asset value.

- Email Authentication – the count of email-related domains that do not implement DKIM or SPF relative to the total population of domains. Weight 50%.
- Email Encryption – the count of email servers that do not implement email encryption relative to the total population of email servers. Weight 50%.
- Email Hosting Providers – information only.

DNS Security – Domain Weight: 6.25%
The DNS security domain rating is calculated based on the count of domains missing domain hijacking protection relative to the population of domains, factoring in domain value.

Network Filtering – Domain Weight: 10%
The network filtering domain rating is the lowest rating between the two criteria of unsafe network services and IoT devices.

- IoT Devices – the count of IoT devices exposed to the internet relative to the size of the internet footprint. If any IoT device is discovered, maximum possible rating is 7.4.
- Unsafe Network Services – the count of unsafe network services relative to the size of the internet footprint. If any unsafe network service is discovered, maximum possible rating is 7.4.

Step 3: Calculate Weighted Average Domain Ratings

After the ratings are calculated for each domain, the weighted average ratings for each domain are calculated using the weights shown in the table below and listed in Step 2.

Domain	Weight	Example Rating	Weighted Example Rating
Software Patching	30.00%	10	3.000
Application Security	12.50%	3.4	0.425
Web Encryption	12.50%	1.4	0.175
Network Filtering	10.00%	10	1.000
Breach Events	10.00%	10	1.000
System Reputation	7.50%	10	0.750
Email Security	6.25%	7.8	0.487
DNS Security	6.25%	10	0.625
System Hosting	5.00%	10	0.500
Total	*100.00%*	**Weighted Avg**	7.96

Step 4: Apply Low Rating Factor to Select Domains

In analyzing breach and destructive ransomware events, victims commonly have poor performance in one or more of the areas of software patching, network filtering, application security, or web encryption. To reflect the heightened risk exposure correlation for poor performance in these domains, an additional weighting is applied for D or F ratings, prior to their incorporation in the overall rating. This weighting is used only for calculation of the overall score but does not impact the display of the domain score itself. The following downward adjustments are made for purposes of calculating the overall rating.

Domain	Condition	Adjustment
Software Patching	Rating is D or F	-1.5 from domain rating, minimum allowed value of 0
Network Filtering	Rating is D or F	-1.5 from domain rating, minimum allowed value of 0
Web Encryption	Rating is D or F	-0.8 from domain rating, minimum allowed value of 0
Application Security	Rating is D or F	-0.8 from domain rating, minimum allowed value of 0

These adjustments are made in calculating the overall rating only. The ratings displayed at the individual domain level remain the same. For example, if a company has a 5.4 (D) rating for Software Patching, then for purposes of calculating the overall rating, the Software Patching rating component is 3.9. The rating shown for the Software Patching domain will remain 5.4 (D).

Step 5: Calculate Overall Rating

The last step is to calculate the overall rating using a weighted geometric mean. Applying a weighted geometric mean dynamically increases the weight of domains that are below the center, based on the distance from the center. The table below shows an example calculation.

Domain	Weight	Example Rating	Adjusted	Weighted
Software Patching	30.00%	10	10	3.000

Application Security	12.50%	3.4	**2.6**	0.325
Web Encryption	12.50%	1.4	**0.6**	0.075
Network Filtering	10.00%	10	10	1.000
Breach Events	10.00%	10	10	1.000
System Reputation	7.50%	10	10	0.750
Email Security	6.25%	7.8	7.8	0.487
DNS Security	6.25%	10	10	0.625
System Hosting	5.00%	10	10	0.500
Total	*100.00%*	Weighted Average		7.76
		Weighted Geometric Mean		**5.85**

As shown in the table, the weighted geometric mean results in a much lower rating than the weighted average. The benefit of using the weighted geometric mean is that very poor performing domains are not lost in the averaging. This reflects the reality that good enterprise protection requires strong performance across all areas.

Conclusion

RiskRecon makes it easier for you to understand and act on your cybersecurity risks across your entire supply chain. This is in part because RiskRecon simplifies the passively observable cybersecurity hygiene of organizations into a single rating that strongly correlated to risk outcomes and to good cybersecurity risk management as it is instantiated in the real world, making it easy for you to quickly identify the risk hotspots in your portfolio. And every RiskRecon rating is backed by detailed assessments that you share with your suppliers to improve their risk posture and yours.

RiskRecon. Third party risk ratings and assessments that are easy to understand, easy to act on, and custom tuned to match your risk appetite. Scalable to your entire supply chain.