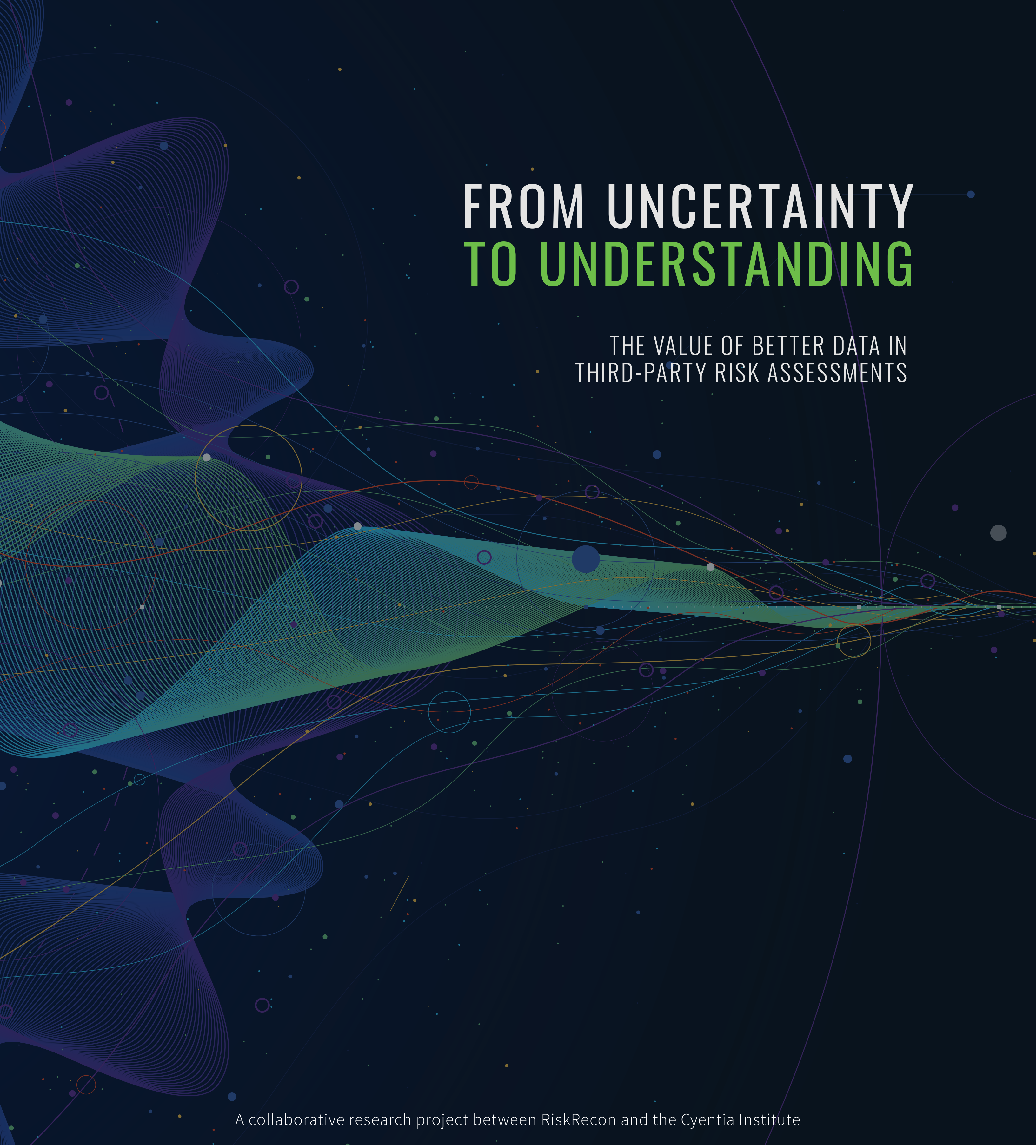
FROM UNCERTAINTY TO UNDERSTANDING

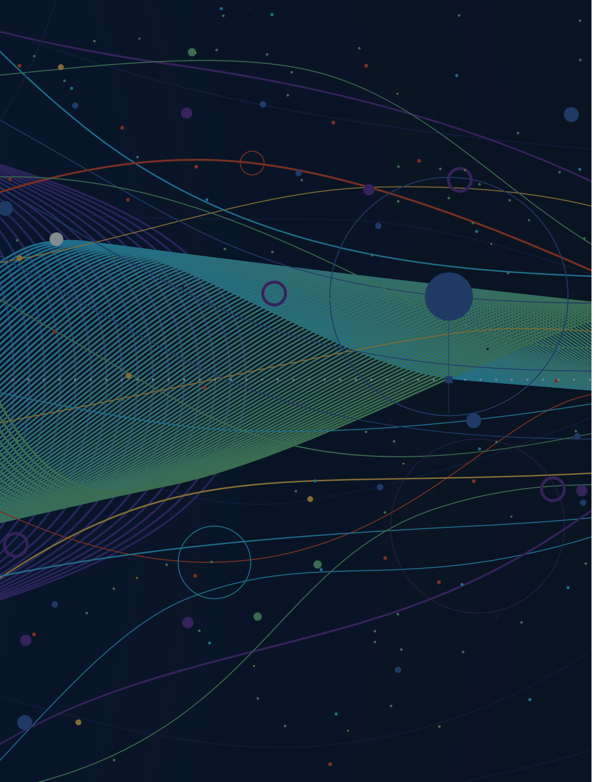
THE VALUE OF BETTER DATA IN THIRD-PARTY RISK ASSESSMENTS



A collaborative research project between RiskRecon and the Cyentia Institute

riskrecon mastercard

119 Cyentia INSTITUTE



We're about to demonstrate how vendor risk assessments based on a full range of technical data collected by RiskRecon provides **22X greater power** for predicting risk posture than using industry as the primary decision factor.

Want to know how? Read on!

HARD DECISIONS DEMAND HARD DATA

"Hindsight's 20/20." You've almost certainly said or heard this phrase before. It's often used in situations when new information comes to light that would have led to different decisions if it had been available at the time. This happens all the time in the field of cybersecurity, especially in third-party risk management (TPRM). TPRM requires triaging a large number of vendors and making critical supply chain risk decisions with imperfect information.

It might be obvious that company in the headlines should have patched that old vulnerability. But that wasn't so clear when they had a thousand other unpatched bugs vying for priority. Sure, it's no surprise that vendor you were nervous about was hacked, exposing sensitive data from hundreds of its partners. But that vendor's last control assessment questionnaire looked no different from any other vendors' answers. There are countless other examples we could use, but the point is clear. Information changes decisions. However, the problem is we don't always have it when we need it.

Decision Theory has a concept called the Expected Value of Perfect Information (EVPI). It's what someone would be willing to pay to get all the information needed to make the best decision in a given situation. Information has value because it eliminates the uncertainty that leads to costly bad decisions and provides the understanding that fuels rewarding good decisions.

The EVPI concept is especially relevant to third-party risk management. Anyone who's performed an internal risk assessment knows that finding data for key cyber risk factors is very challenging. An even greater challenge is trying to assess those same factors across the hundreds and sometimes thousands of other organizations required for TPRM. In that scenario of high uncertainty, information that drives greater understanding is very valuable indeed.

This short study aims to measure the value of better information for third-party risk assessments. We developed four models of increasing information to assess vendor risk posture and compare the power of those models to identify which vendors represent the greatest risk to sourcing organizations. We also determine which specific types of information (i.e., firmographic or technical) are most valuable for these assessments. In the end, you will come away knowing what information is most useful for third-party risk assessments and how much improvement you can expect from having that information.

The dataset used for this report comes from RiskRecon's discovery and analysis of internet-facing systems, domains, and networks to provide customers visibility into their third-party risk. It contains sanitized information on 40,000 organizations of all types and sizes, nearly 9 million assets hosted across 200+ countries, and more than 70 million security findings.

INTRODUCTORY THOUGHTS FROM KELLY WHITE, CEO @ RISKRECON

With enterprises critically dependent on such large and complex supply chains, traditional methods of managing third-party risk simply do not provide the timely, accurate information necessary to scale at business speed. In the face of these realities, what are the protectors of enterprise assets and supply chains to do?

A big part of the answer lies in data. In operating on the Internet, companies cannot help but reveal the quality of their cybersecurity risk management. It shows in their systems, their applications, the signals they emit to the Internet, and the breach events they incur. We at RiskRecon, as a leading provider of cybersecurity ratings and insights, claim that opensource intelligence-based assessments of your vendors and partners enables better risk decisions.

The obvious question is: Does OSINT-based assessment data enable better third-party risk decisions? We engaged Cyentia to answer this question. Of course, Cyentia (or anyone for that matter) does not know the actual risk management quality of a company, so they came up with an objective proxy for what good risk management looks like – the rate of high and critical severity issues in systems that collect sensitive data.

With this proxy in place, Cyentia put their data science magic to work against tens of thousands of companies to see how powerful four different data scenarios were in predicting the rate of high and critical severity issues in the high value systems of each company. They started with just industry information, added additional firmographic information for the next scenarios, and for the final scenario added in the RiskRecon assessment information. In doing so they of course excluded information related to the findings they were seeking to predict.

At the risk of spoiling the paper, I will say this – it is in fact true that OSINT cybersecurity assessment data is very useful in predicting which companies manage risk better. Basic firmographic information, while useful in comparing one industry to another, is not useful in assessing the risk quality of a specific company. The OSINT cybersecurity assessment data has a 21.7-times greater predictive power than does basic firmographics.

It boils down to this – do you want to do business with vendors and partners who maintain a low rate of high and critical severity issues in their sensitive systems? A broad spectrum of firmographic information won't give you the answer. The data behind our cybersecurity ratings will. It will help you manage your third-party and supply chain risk better and faster.

Please enjoy reading the study. Cyentia does great work.

TABLE OF CONTENTS

MEASURING CYBER RISK POSTURE................4

PREDICTING CYBER RISK POSTURE................6

COMPARING PREDICTION MODELS....13

BRINGING CLARITY TO UNCERTAINTY...........14

riskrecon mastercard

RiskRecon enables clients to easily understand and act on their third-party risk through cybersecurity ratings and continuous security control assessments.

MEASURING CYBER RISK POSTURE

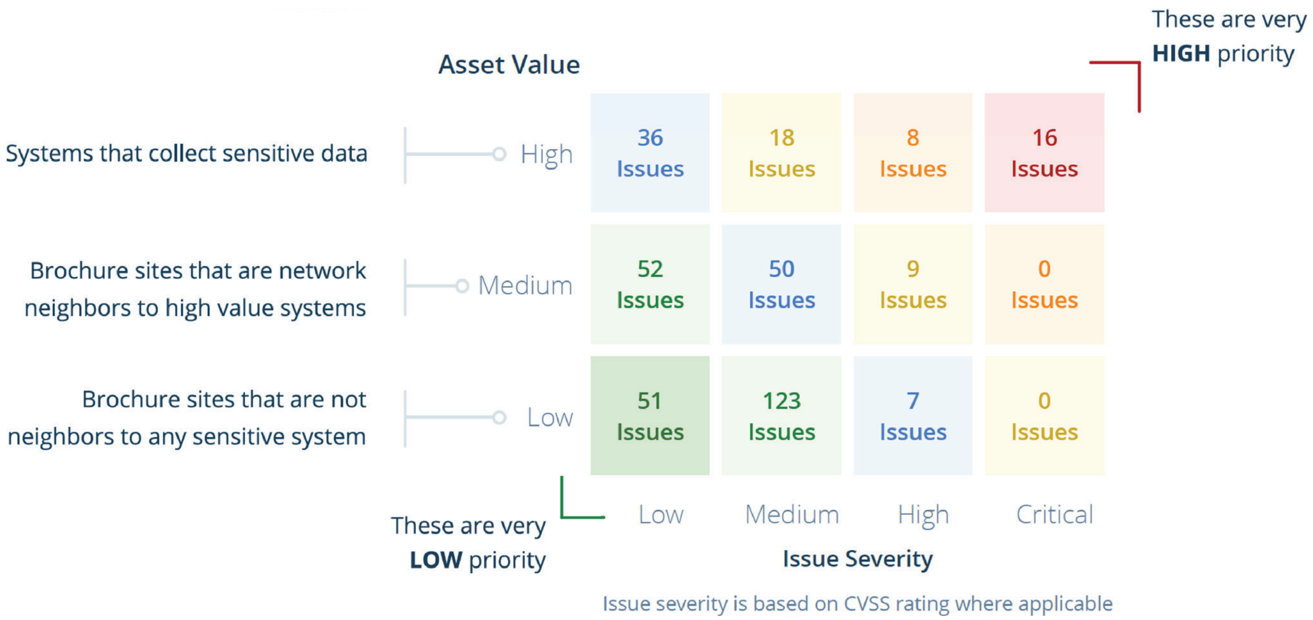
In a perfect world, third-party risk managers would be able to accurately and continually assess expected losses associated with each vendor in their supply chain. Sadly–that is not our reality. In turn, what we do have is a reasonable proxy for organizational cyber risk posture that meets the needs of this analysis and risk managers.

While we all know that firms with strong security defenses can still suffer major losses (and the weak but lucky ones might squeak by with none), experience shows that firms that manage risk well perform better over the long term. We've chosen to use the density of high and critical security findings affecting high-value assets as a measurable proxy for organizational cyber risk posture in our prediction models.

This measure of risk posture incorporates two key dimensions from RiskRecon's dataset, as depicted in Figure 1:

1. **Security Findings:** Detection of security-relevant issues that expose hosts to various threats. We focus on findings rated high or critical in severity according to the Common Vulnerability Scoring System (CVSS).

2. **Asset Value:** Relative sensitivity and criticality of hosts based on multiple indicators. We focus on high-value assets, which collect sensitive data, authenticate users, run critical services, etc.



These are very **HIGH** priority

Asset Value		Low	Medium	High	Critical
Systems that collect sensitive data	High	36 Issues	18 Issues	8 Issues	16 Issues
Brochure sites that are network neighbors to high value systems	Medium	52 Issues	50 Issues	9 Issues	0 Issues
Brochure sites that are not neighbors to any sensitive system	Low	51 Issues	123 Issues	7 Issues	0 Issues

These are very **LOW** priority

Issue Severity

Issue severity is based on CVSS rating where applicable

Figure 1: RiskRecon's Risk Prioritization Matrix for security issues

Notably, this approach isn't just an empty marketing scheme; it's consistently reinforced by our research with RiskRecon. For example, our [investigation of Internet of Things](#) (IoT devices) from 2020 found a 70x jump in the rate of critical security issues in high-value assets between organizations that expose vulnerable IoT devices to the internet vs. those that do not. Organizations that cannot manage the critical security issues affecting their most valuable assets are almost certainly struggling with many aspects of managing their cyber risk posture.

The idea here is simple. We ultimately want to answer the question "How risky is this vendor relative to others?" If a vendor isn't addressing the most severe security issues in their most valuable assets, they're probably not managing risk posture in a way that sustains good performance. At the very least, they wouldn't be your first choice for entrusting privileged access to your systems and data.

But there's one more thing we need to do to enable proper comparisons of risk posture across all organizations. We must calculate the density of high and critical security findings in high-value assets on a per-host basis, normalizing firms of varying size and findings. Then we can examine how organizations in our sample perform according to our risk posture measure in Figure 2.

Here we see most organizations have less than one high or critical finding per high-value host. But there's a subset of firms that have a much higher risk density. It's this subset of high risk vendors that we want to identify in our TPRM portfolio.

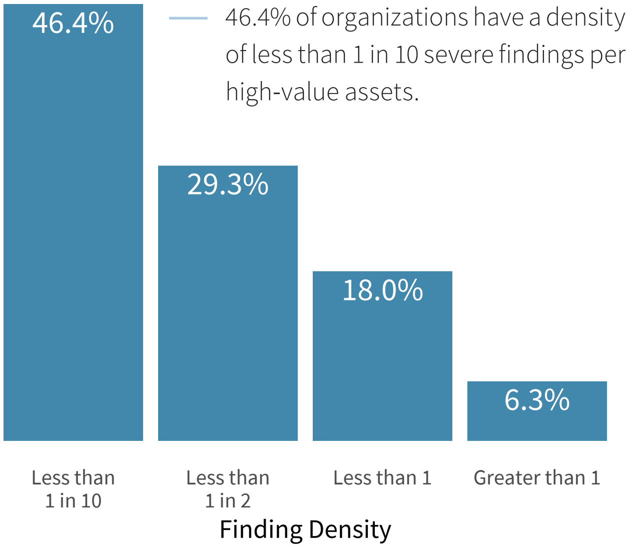


Figure 2: Density of high and critical security issues per high-value asset across organizations

IMPORTANT NOTE ON OUR PROXY FOR ASSESSING RISK POSTURE

We're using the number of high and critical security issues affecting high-value assets as a proxy for risk posture. Our research has repeatedly shown that organizations failing to address the worst security issues in their most valuable assets are also struggling with many other aspects of managing cyber risk.

PREDICTING CYBER RISK POSTURE

With our measure of risk posture defined and normalized, we can get down to the business of finding the factors that provide a reliable signal of an organization's cyber risk posture. To make this more than an impersonal analytical exercise, we've decided to simulate decision scenarios that will be familiar to most readers by attempting to figure out which vendors are more likely to pose cause trouble in the form of cyber incidents and losses.

- Scenario 1: Industry only
- Scenario 2: Basic firmographics
- Scenario 3: Hosting profile
- Scenario 4: Full technical insight

We begin with two trivial scenarios where only very basic firmographic information is available on which to base third-party risk assessments. The third scenario adds some additional information about the vendor's IT infrastructure to (hopefully) better peg risky vendors. Our final scenario incorporates the full technical details available in RiskRecon's continuous monitoring dataset to support decision making.

For each scenario, we built a predictive model using the risk posture measure described above as our dependent (outcome) variable. Factors included in each scenario/model are described below, along with the strength of their contribution (or lack thereof) to the predictive model. We'll assess each model's performance individually and show how each step up in information increases our ability to make better decisions.

SCENARIO 1: INDUSTRY ONLY

Let's first revisit a key finding from our Internet Risk Surface Report. In that report we demonstrated that industries have different levels of risk exposure in the aggregate. A busy TPRM professional may be tempted to lump firms into risk categories based on their industry. This 'Industry-Only' determination is our first scenario.

An immediate practical problem with this approach is that it's rare that an organization can decide between doing business with a firm in, for example, the hospitality industry versus one in the energy sector . While industries differ in broad population, risk practitioners need to decide between a number of different individual firms to help their organization carry out their business functions. And at the individual firm level there is a lot of variation between the best and worst performers in each industry. In Figure 3 below, we show the median density of severe findings among high-value assets for each industry. We also display the range of finding densities found across firms in each industry, showing two-thirds of the overall spread.

> Interested in the nerdy details of the models we've built? For each scenario we created a linear regression to explain the effects of various factors upon the logged flaw density (high/critical findings on high-value hosts). Our objective is to find correlations and explanations within the organizations present in our dataset, This allows us to focus on the statistical significance of predictive factors rather than the effect size.

Notice how the dot indicating the median is clearly different in Figure 3, but the bars showing the range of common values for individual firms overlap. This tells us that, in general, the education sector tends to have a worse risk posture than the finance sector, but many individual financial firms are equally or riskier than educational institutions. More rigorously, a risk manager using only industry to determine the risk of an individual firm can only explain 2.8% of the variation among all the firms (see Figure 4). Thus, this model results in extremely unreliable predictions (yet we often hear and cringe - of organizations using industry as the primary variable in their risk assessments and models).

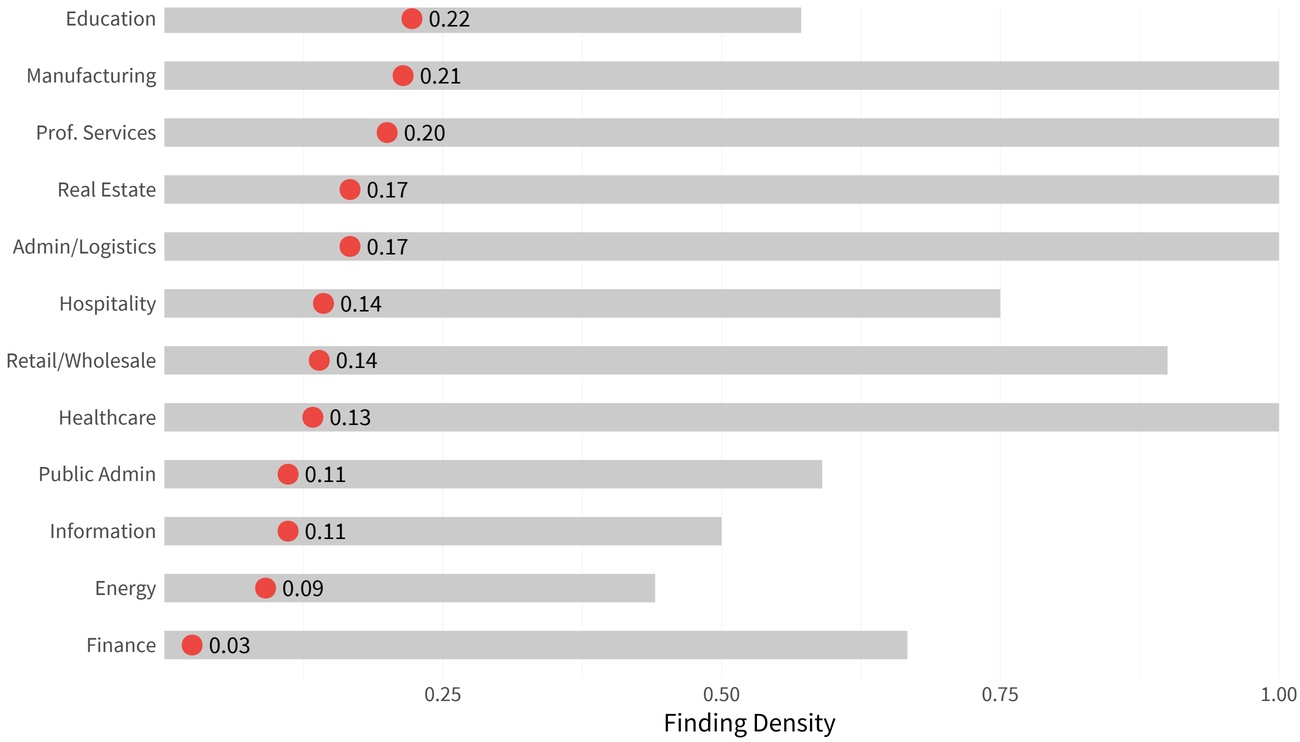


Figure 3: Comparison of the density of high and critical security issues in high-value assets by industry (median in blue)

It is clear a model that can only explain 2.8% of what determines a firm's risk posture isn't one we'd suggest anyone seriously employ. But it's a simple demonstration of the problems of trying to zoom in to the potential risk of a specific firm. This problem continues even as we try to add more information and build up to a more realistic model.

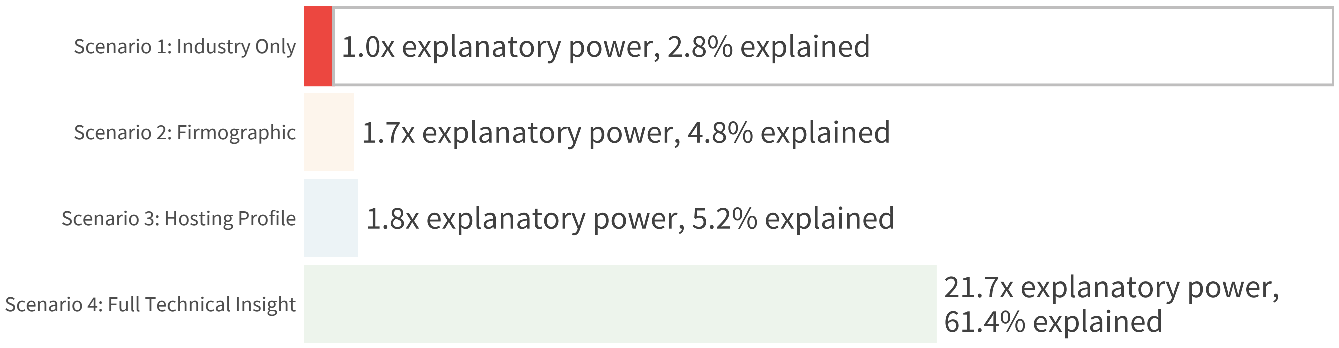


Figure 4: Explanatory power (R^2 statistic) of a risk posture prediction model based solely on a firm's industry

SCENARIO 2: BASIC FIRMOGRAPHICS

In our second scenario, we expand beyond industry but still limit our third-party risk manager to only basic firmographic elements about vendors, namely industry, organization size, and primary country of operation. This information is readily available prior to any kind of technical assessment. On a small scale, these data points can be gleaned simply by knowing the company. On a larger scale (i.e., across an entire vendor portfolio), services like Dun & Bradstreet and Hoovers supply this level of information.

Features Used

Scenario 2 - Basic Firmographics

FEATURE	DESCRIPTION
Industry	*Industry as used in the first scenario.*
Organization Size	Size of the organization (measured by number of visible hosts).
Primary Country	Majority country of internet presence.

Table 1: Firmographic features added to the risk posture prediction model for this scenario

Using this information, we re-constructed our model using our risk posture proxy of the density of high and critical findings on high-value assets as the outcome variable. The chart below shows the firmographics that have the greatest effect on risk posture predictions and whether they indicate lower risk (extending to the right) or higher risk (extending to the left).

These results give our third-party risk professional some basis for considering manufacturing firms based in India as more "risky" and thus deserving of more attention. Conversely, there's evidence that firms in the banking sector, as well as those located in the United States, might be reasonably deprioritized if time or resources are limited.

This is a really weak model built for illustrative purposes.

Do not make any decisions based on what you see here!

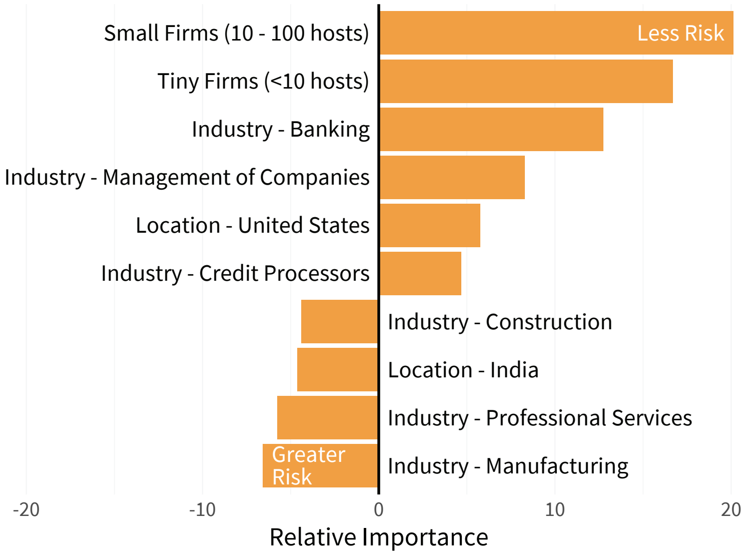


Figure 5: Relative importance of features included in the risk posture prediction model for this scenario

In conclusion, the overall predictive strength of the 'Firmographic Only' model is quite weak. The R2 is less than 4.8%, indicating firmographics alone explain less than five percent of the variation in a firm's risk posture. That's not very helpful to third-party risk practitioners needing reliable insight. Practically, that means the chance of misjudging the potential risk associated with vendors (and thus mis-assigning control requirements) is very high. Let's see how we can improve our odds by feeding more information into the model.

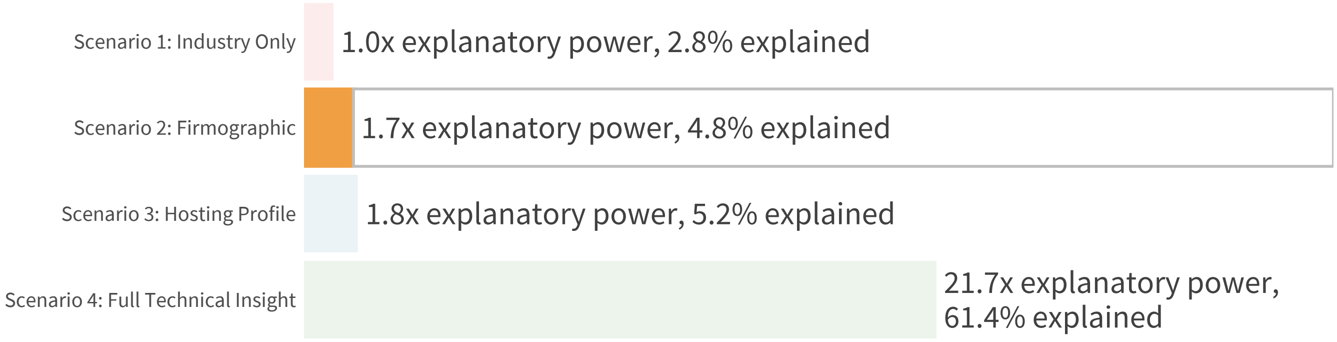


Figure 6: Explanatory power (R^2 statistic) of the risk posture prediction model for this scenario

SCENARIO 3: HOSTING PROFILE

Now let's give our third-party risk manager access to additional information about the external hosting profile of a vendor. Whether through an initial onboarding process or some additional investigation, there's now visibility into risk factors like the geographic distribution of hosts, the proportion of hosts running sensitive or critical functions, and the allocation of hosts across on-prem vs. cloud environments.

Features Used

Scenario 3 - Hosting Profile

FEATURE	DESCRIPTION
Industry and Firmographics	*All features from the previous two scenarios.*
Cloud Percentage	Proportion of an organization that is in the cloud.
Geographic Diversity	Number of countries where an organization has hosts.
Proportion of High Value Host	Density of high value hosts in an organization's external surface.

Table 2: Internet infrastructure features added to the risk posture prediction model for this scenario

Adding these hosting elements to the existing firmographic factors and constructing a new model based on both changes a few things, but doesn't change the overall outcome very much. There's still justification for revising risk assessments down for financial services firms and up a bit for professional services and manufacturers. Interestingly, we now begin to see some differentiation with organization size. Small and tiny firms still appear less risky (for now).

Specific to the new hosting variables, only the number of hosting countries shows up as an important new variable. Even though the new factors don't make a huge difference in the final outcome, they are still significant in the model by how they influence pre-existing factors. Notice how the importance of being located in India disappears as a determinant of risk. This is not surprising as country has many of the same characteristics as industry – lots of variation of risk in the aggregate, but not necessarily predictive at the individual firm level.

Although a little better, this still isn't a good model.

Notice old factors begin to shift as new ones are brought into the model.

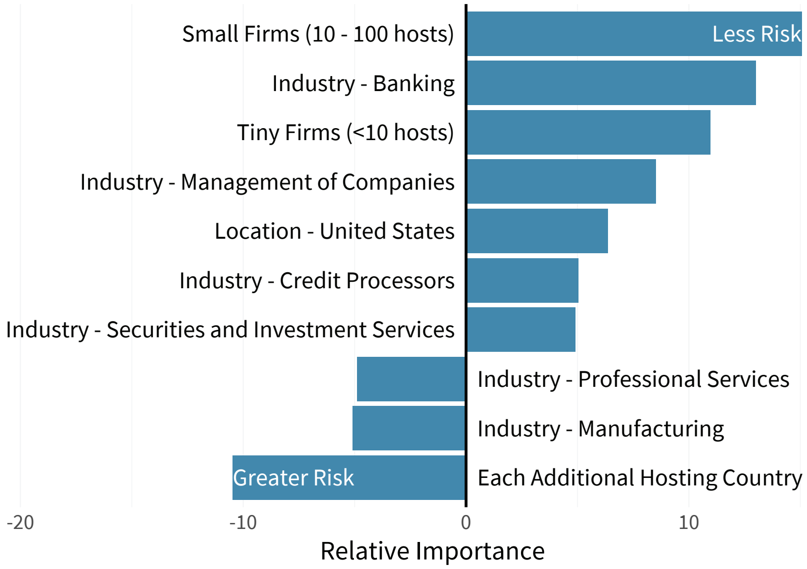


Figure 7: Relative importance of features included in the risk posture prediction model for this scenario

But like we said—these shifting variables don't change much about the predictive power of this model. The R2 statistic barely nudges up to 5.2%, so our third-party risk manager still faces a huge amount of uncertainty in trying to separate the wheat from the chaff across the vendor portfolio. We'll give it one more try to build a better model that offers some actionable insight.

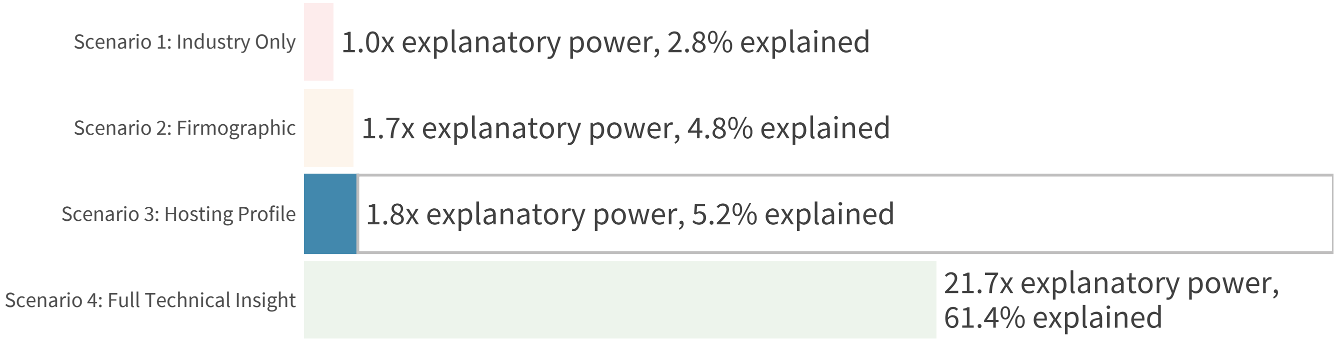


Figure 8: Explanatory power (R^2 statistic) of the risk posture prediction model for this scenario

SCENARIO 4: FULL TECHNICAL INSIGHT

In this final scenario, we assume that our third-party risk manager now has access to the full suite of RiskRecon cybersecurity ratings and insights. This includes all the firmographic and infrastructure dimensions of previous models plus detailed reporting on the volume and variety of security issues discovered by RiskRecon across Internet-facing hosts. Such issues include the presence of exposed network services, unpatched software vulnerabilities, configuration and authentication problems, and other findings falling under the categories shown below.

Features Used

Scenario 4 - Full Technical Insight

FEATURE	DESCRIPTION
Industry, Firmographics, and Internet Infrastructure	*All features from the previous scenarios.*
Application Server Patch Findings	Are there hosts with missing application security patches?
CMS Authentication Findings	CMS authentication problems.
Content Management Systems Patch Findings	Are there CMS security patches missing?
High Value Systems Encryption Findings	Are high value systems have missing network encryption?
IOT Devices Present	Are there IOT systems in the external attack surface.
Miscellaneous Patch Findings	Other security-related patching findings.
OpenSSL Patch Findings	Are there unpatched OpenSSL instances.
Operating System Patch Findings	Are there hosts with missing OS security patches?
Unsafe Network Services	Are unsafe services deployed in an unsecured state?
Web Server Patching Findings	Are there web servers with missing patches?

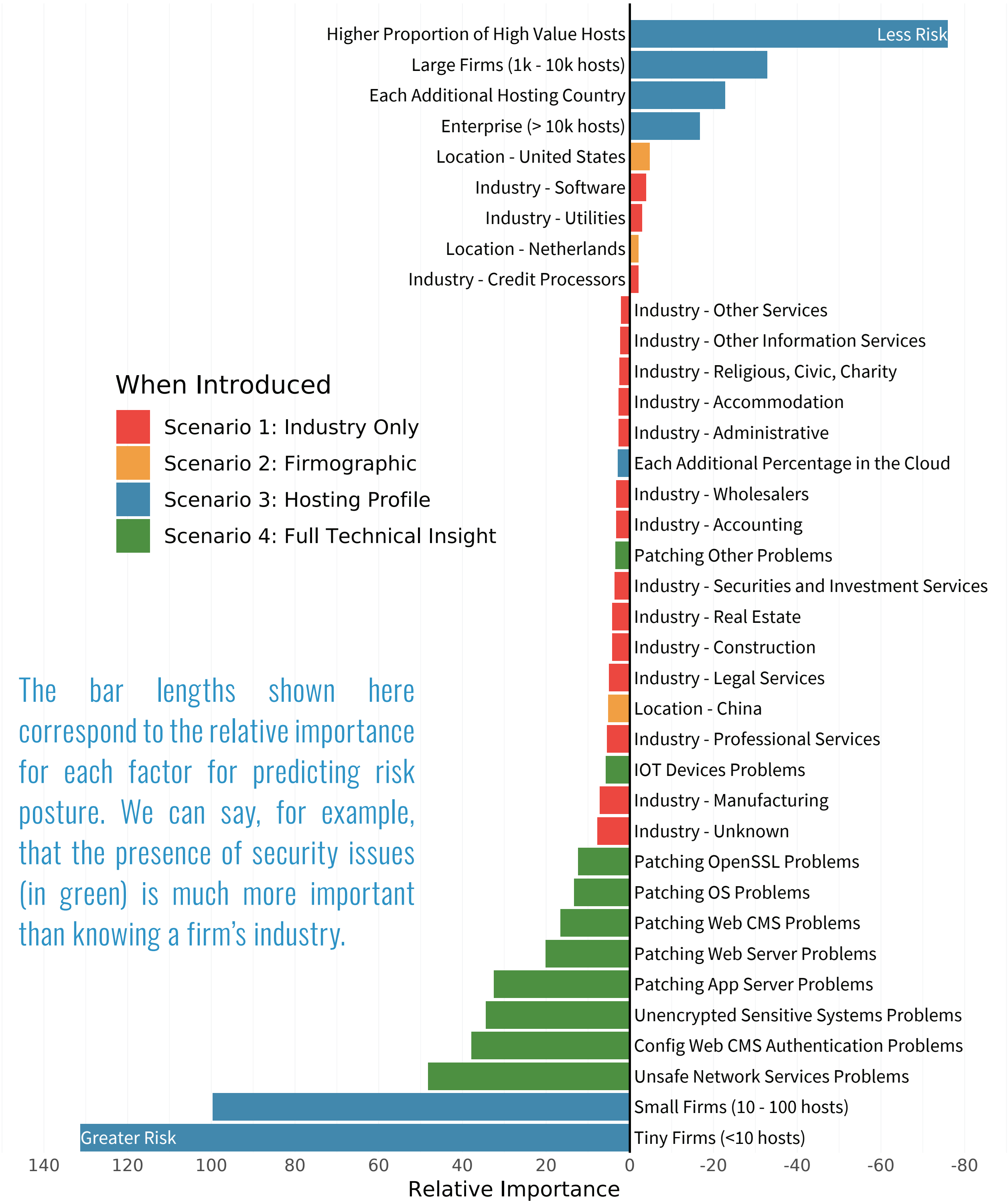
Table 3: Technical features assessed by RiskRecon added to the risk posture prediction model for this scenario

Yes, we're using security findings to predict security findings, but we've eliminated high and critical findings on high-value assets from our set of predictor variables because those represent what we're trying to predict.

In this new high-fidelity model shown in Figure 9, we see a radical shift in what matters most. Things that drove perception of vendor risk in prior models, such as industry and primary country, now become largely irrelevant. Even cloud adoption and geographic distribution of hosts don't contribute much to our understanding of risk. How organizations manage the security of their infrastructure—wherever it's located—has a much stronger effect on vendor risk posture.

This doesn't mean that the primary country isn't an important risk factor. It simply means physical geography isn't nearly as important when you have detailed insight into actual security findings. In other words, it would not be wise to say, "this vendor has a ton of security findings but they're a U.S. software firm, so we'll give them a pass." **Bottom line: what you do is a much bigger determinant of risk than who you are.**

It's curious that a smaller firm size predicts greater risk in Figure 9 but indicated less risk in the earlier scenarios. That's a common occurrence in models and decision-making in general. As new information comes to light, the old information is reassessed and potentially weighted differently than before. Specific to this model, once you know what's really going on with security findings, you have more clarity on how size and other firmographics actually impact risk.



The bar lengths shown here correspond to the relative importance for each factor for predicting risk posture. We can say, for example, that the presence of security issues (in green) is much more important than knowing a firm's industry.

Figure 9: Relative importance of features included in the risk posture prediction model for this scenario

Even with that explanation, the huge relative importance of organization size in this "Everything Model" is rather hard to process. Our best interpretation of what's going on here is that once we have a proper assessment of security-related issues, organization size (which often correlates with resources) becomes a major predictor of a vendor's ability to address those issues. According to the data underlying this model, smaller firms tend to struggle to fix security issues, whereas larger enterprises—even though they often have more findings—are able to mitigate them in a timely manner.

With respect to the various types of security findings assessed, exposing unsafe network services proved to be the strongest single predictor of risk posture. That's rather serendipitous because we published an entire report detailing the prevalence and effect of such services. What we see here echoes what we learned there: organizations that tend to be laxer in controlling unsafe services also tend to exhibit wider security issues.

We won't elaborate on all of the remaining findings individually but suffice it to say that validating vendor security hygiene using factors like those shown in green in Figure 9 goes a long way toward building a proper understanding of their risk posture. These technical insights provide a focusing lens so that other information, such as firmographics, can be used with greater power and precision. It's easy to answer "Yes" to a questionnaire asking whether all systems and applications are updated. But it's not so easy to bluff when the cards are face up on the table.

COMPARING PREDICTION MODELS

More important than any individual contributing factor is the overall strength of this model. The proof, as they say, is in the pudding. To that end, Figure 10 offers a blind taste test to see which pudding model works best for predicting vendor risk.

Recall that our firmographic model posted an R^2 of 0.048. Adding the infrastructure variables nudged that up to 0.052. To put that into perspective, imagine trying to make a critical life decision if you knew just 5% of the things that would ultimately spell success or disaster. Not very helpful, right?

Well, thankfully, having visibility into the security posture of a vendor's systems is a lot more helpful in making good decisions. The 'full technical insight' model discussed in the previous section achieved an R^2 of 0.614. That's nearly 22 times more effective for diagnosing vendor risk posture than relying on industry information alone!

We now come full circle to the chart from the beginning of this report. We trust that you can now see the ineffectiveness of the first three scenarios when it comes to determining a prospective partners risk surface.

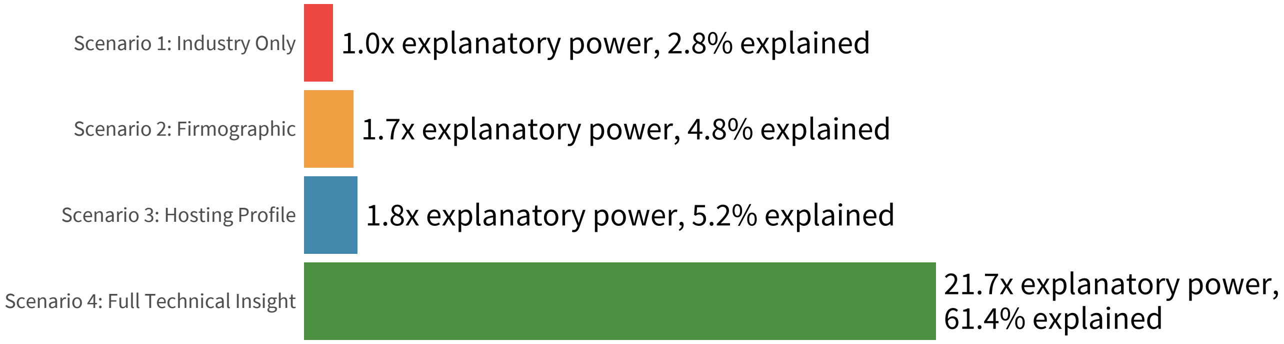


Figure 10: Comparing explanatory power (R^2 statistic) of risk posture prediction models for the four scenarios evaluated

BRINGING CLARITY TO UNCERTAINTY

Enterprises are critically dependent on large and complex supply chains. Events at vendors and even at companies deeper in the supply chain can result in theft of assets or interruption of the ability to operate. The reality is that, while the protection of assets and services you have placed in the hands of your supply chain, the risk remains yours. You can outsource your systems and services, but you can't outsource your risk.

GOOD DATA YIELDS GOOD RISK MANAGEMENT

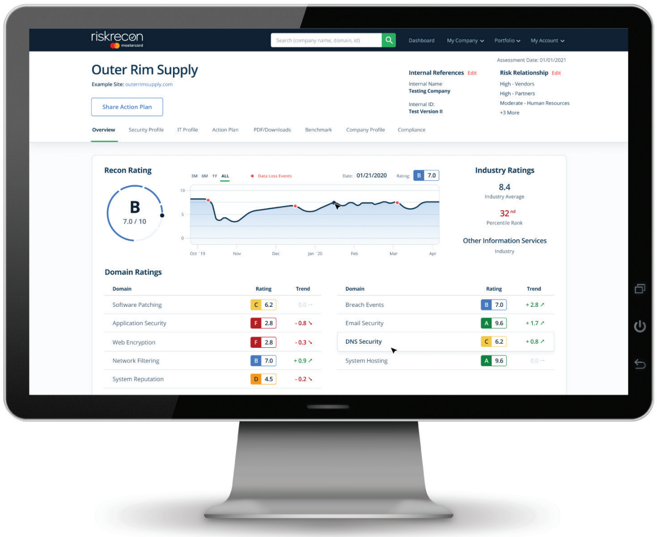
Managing risk well requires good data. It is necessary for managing your internal enterprise risks and is just as necessary for managing your supply chain risks. How do you know if a new vendor is going to protect your risk interests well? How do you know if your current vendors – it could be tens, hundreds, or even thousands – are protecting your risk interests well? How do you know if a data breach or a critical vulnerability will impact you through your supply chain? Luckily, there is a solution that provides you with the visibility you need to make third-party cyber risk decisions and take action swiftly.

RiskRecon provides cybersecurity ratings and insights that make it easy to understand and act on your cybersecurity risks. Its accurate, automated, and actionable technology allows you to get both the situational and detailed assessment insight necessary to better manage the risk of your internal and extended enterprise across your risk decisions and operations.

FREE OFFER: KNOW YOUR 3PTY SECURITY RISKS

As a busy third-party risk professional taking swift action with limited information is no easy feat. Fortunately, RiskRecon is offering complimentary enterprise access to assess and monitor the cybersecurity of your supply chain for 30 days.

For 30 days you can enjoy a detailed view of the risk up to 50 vendors pose to your organization. Plus, you'll learn how to use these scores to influence corrective action with risk prioritized data based on issue severity.



Outer Rim Supply

Example Site: outerrimsupply.com

Assessment Date: 01/01/2021

Internal References Edit

Internal Name
Testing Company

Internal ID:
Test Version II

Risk Relationship Edit

High - Vendors
High - Partners
Moderate - Human Resources
+3 More

Recon Rating

B
7.0 / 10

Date: 01/21/2020 Rating: B 7.0

Industry Ratings

8.4
Industry Average

32nd
Percentile Rank

Other Information Services
Industry

Domain Ratings

Domain	Rating	Trend	Domain	Rating	Trend
Software Patching	C 6.2	0.0 →	Breach Events	B 7.0	+ 2.8 ↗
Application Security	F 2.8	- 0.8 ↘	Email Security	A 9.6	+ 1.7 ↗
Web Encryption	F 2.8	- 0.3 ↘	DNS Security	C 6.2	+ 0.8 ↗
Network Filtering	B 7.0	+ 0.9 ↗	System Hosting	A 9.6	0.0 →
System Reputation	D 4.5	- 0.2 ↘			

What's included in the offer?

- Detailed assessment of your own IT assets
- Security ratings and summary assessment of up to 50 vendors
- Full access to RiskRecon Technical Support
- A risk-prioritized view into your vendor ecosystem with our vulnerability matrix
- Superior data accuracy (over 99% - which drastically reduces false positives)

Register to get insights into your supply chain at https://www.riskrecon.com/know-your-portfolio.

RiskRecon enables clients to easily understand and act on their third-party risk through cybersecurity ratings and continuous security control assessments.

www.riskrecon.com

The Cyentia Institute produces compelling, data-driven research with the aim of improving knowledge and practice in the cybersecurity industry.

www.cyentia.com

A collaborative research project between RiskRecon and the Cyentia Institute