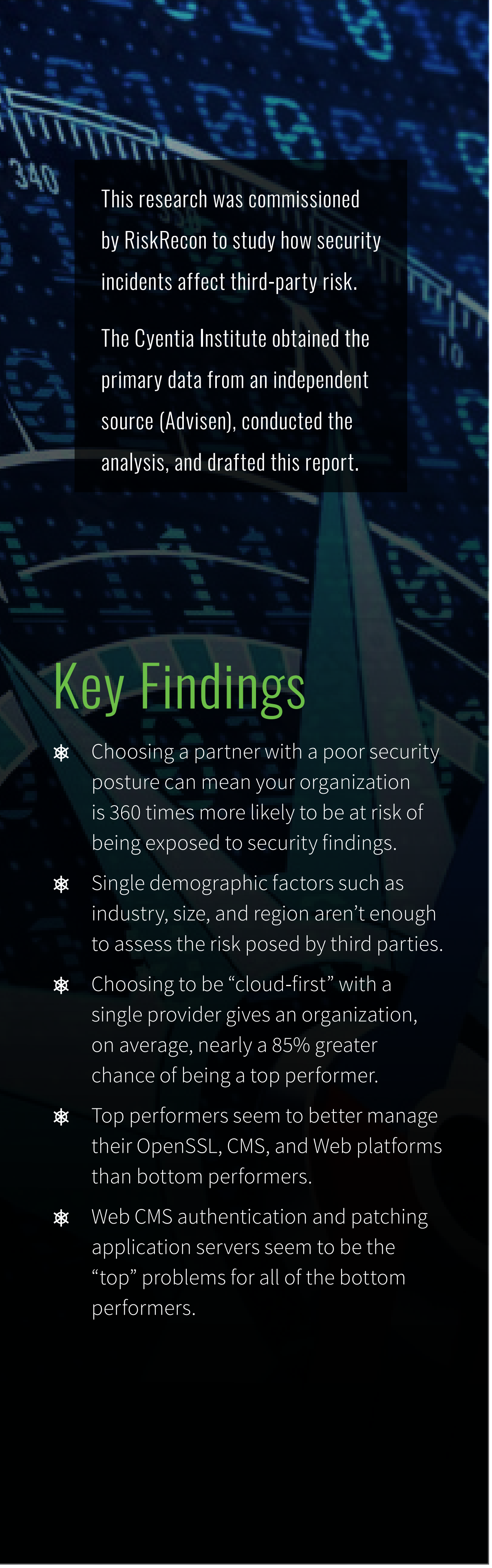
NAVIGATING THE INTERNET RISK SURFACE

A COLLABORATIVE RESEARCH PROJECT BETWEEN RISKRECON AND THE CYENTIA INSTITUTE

riskrecon

mastercard

119 Cyentia INSTITUTE



This research was commissioned by RiskRecon to study how security incidents affect third-party risk.

The Cyentia Institute obtained the primary data from an independent source (Advisen), conducted the analysis, and drafted this report.

Key Findings

- Choosing a partner with a poor security posture can mean your organization is 360 times more likely to be at risk of being exposed to security findings.
- Single demographic factors such as industry, size, and region aren't enough to assess the risk posed by third parties.
- Choosing to be "cloud-first" with a single provider gives an organization, on average, nearly a 85% greater chance of being a top performer.
- Top performers seem to better manage their OpenSSL, CMS, and Web platforms than bottom performers.
- Web CMS authentication and patching application servers seem to be the "top" problems for all of the bottom performers.

TABLE OF CONTENTS

HAVE COMMENTS OR QUESTIONS ABOUT THIS REPORT?

We'd be glad to discuss them. No, really—we love this stuff! RiskRecon and the Cyentia Institute can be reached via the methods shown below.

RiskRecon: info@riskrecon.com or @riskrecon on Twitter

Cyentia: research@cyentia.com or @cyentiainst on Twitter

INTRODUCTION

"We shall not cease from exploration...
and the end of all our exploring
will be to arrive where we started...
and know the place for the first time."
- T.S. Eliot, "Little Gidding"

The world is complex, and ultimate control may be beyond our individual grasp; yet our decisions – what we eat, where we go, how we do business, and why we turn in one direction instead of another – still matter. In business, choosing to partner with one company or another is a decision that firms regularly make, and those decisions can have a profound effect on the risk that the sourcing firm is exposed to.

When managing risk, making binary assumptions, -- either something is good (safe) or bad (unsafe) -- is tempting. To get on with the business of business and not be paralyzed with perpetual analysis, we have to make informed decisions about the risks and benefits that a business relationship entails. This must be done by understanding not only the potential consequences for an organization but also for that organization's network of vendors, suppliers, customers, and employees.

In this risk surface series, RiskRecon, a Mastercard Company, and Cyentia have worked to help third-party risk managers understand how to measure and manage risk. We've seen variation across industries and other slices. But not all firms are interchangeable. A payroll processor cannot be replaced with a janitorial supply company, at least not with good business outcomes! In this report, we look at what distinguishes top-performing firms from those that struggle the most. Armed with this knowledge, Third-Party Risk Management (TPRM) professionals can take into account the totality of their risk surface, and how it impacts the overall security performance of an organization.

As discovered in our previous report on third party risk management, 1 in 3 programs assess over 100 vendors per year. And they have good reasons to do so.

We first decided to take a look at the typical number of high-value findings found on high-value hosts. On average, a bottom-performing organization has 360 times (yes, 36,000%) more high value findings than a typical top-performing partner.

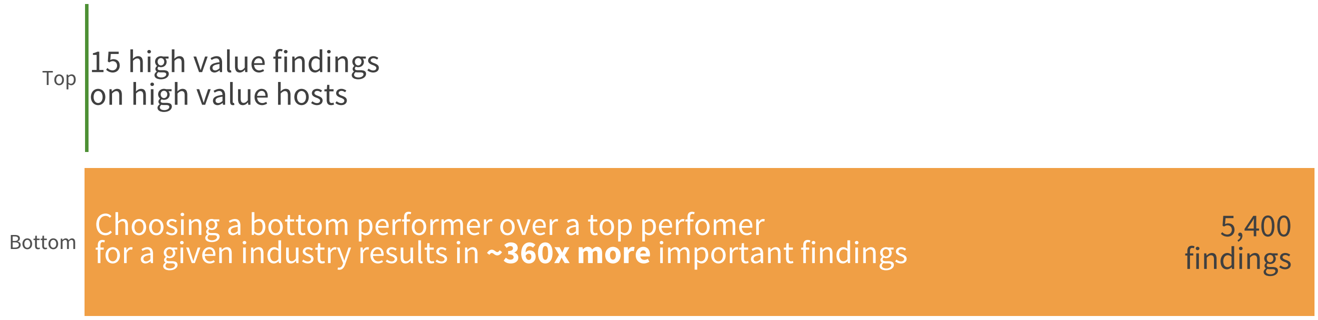


FIGURE 1: DIFFERENCE IN KEY FINDINGS WHEN CHOOSING A BOTTOM PERFORMER VS. A TOP PERFORMER

Against this backdrop, throughout this report, we'll not only define how we identify top and bottom performers in terms of high risk, but we'll also dive deeper into what divides the two bookend performers in terms of key performance indicators that influence their risk surface.

THE DATASET FOR THIS REPORT COMES FROM A SAMPLE OF 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 THOUSANDS OF ORGANIZATIONS OF ALL TYPES AND SIZES, COVERING MILLIONS OF ASSETS HOSTED ACROSS 228 COUNTRIES, AND NEARLY HUNDREDS OF MILLIONS OF SECURITY FINDINGS.

WHAT'S "RISK SURFACE"?

Let's briefly recap what "risk surface" is. A company's risk surface refers to anywhere an organization's ability to operate, reputation, assets, legal obligations, or regulatory compliance is exposed to risk. The aspects of a firm's risk exposure that is associated with or is observable from the internet is considered its internet risk surface. Given that a huge portion of a modern organization's value-generating activities relies on internet-enabled processes and third-party relationships, its risk surface is much more extensive than one might expect.

There are many things that can be measured about an organization's internet risk surface based on the broad definition above. In the first edition of the Internet Risk Surface Report, our exploratory analysis focused on the following five key dimensions:

RISK SURFACE

ANYWHERE AN ORGANIZATION'S ABILITY TO OPERATE, REPUTATION, ASSETS, LEGAL OBLIGATIONS, OR REGULATORY COMPLIANCE IS EXPOSED TO RISK.

HOSTS The number of internet-facing assets associated with an organization.

VALUE The relative sensitivity and criticality of hosts based on multiple indicators.

PROVIDERS The number of external service providers used across hosts.

GEOGRAPHY A measure of the geographic distribution of a firm's hosts.

FINDINGS The security-relevant issues that exposed the hosts to various threats.

IN THIS EDITION OF THE RISK SURFACE REPORT

WE BRING THESE DIMENSIONS FORWARD AND EXPLORE THEM IN NEW WAYS WHILE ADDING SOME NEW ANGLES. OUR MAIN FOCUS IS LESS ON THE MEASURES THEMSELVES AND MORE ON HOW THEY IMPACT THE ENTERPRISE'S CYBERSECURITY POSTURE AND THIRD-PARTY RISK.

IN PARTICULAR, WE SEEK TO UNDERSTAND HOW THE TOP AND BOTTOM PERFORMING ORGANIZATIONS DIFFER ACCORDING TO THESE MEASURES.

DEFINING AND IDENTIFYING TOP & BOTTOM PERFORMERS

I've got one, two, three, four, five
Senses working overtime
Trying to taste the difference
'tween a lemon and a lime
XTC, Senses Working Overtime

Before we can identify what separates the top and bottom performers, we need to define what "top" and "bottom" mean. How do we place any given organization in one category or the other? While business performance metrics abound, here we're focused solely on how well organizations manage their cybersecurity posture. Our primary measure for well-performing organizations is the same as used in our Uncertainty to Understanding report, i.e., high-risk findings density.

BY FOCUSING ON WHAT MATTERS MOST (HIGH AND CRITICAL FINDINGS ON HIGH VALUE ASSETS) ORGANIZATIONS CAN DIRECT EFFORTS WHERE THEY WILL HAVE THE BIGGEST IMPACT.

We used a large sample of data from RiskRecon, filtering it down to organizations that have at least 50 active hosts. This means that this sample represents significantly sized firms to help shift our focus to organizations with not only a more prominent digital footprint but also those that were more likely to be candidates for enterprise-level partners. We then identified organizations with the highest and lowest proportion of high-risk findings density. The top performers, which are the organizations with the lowest finding density, caused a little wrinkle for us, since many of these organizations had no findings. Thus, the top performers considered for the present purpose have a high-risk finding density of zero as well as a RiskRecon score of A.

HIGH-RISK FINDINGS DENSITY

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

While it's true that firms with strong security defenses can still suffer major losses (and those with weak defenses may, through luck, squeak by without experiencing any), experience shows that firms that manage risk well perform better over the long term. Thus, we use the density of high and critical security findings that affect high-value assets as a measurable proxy for organizational cyber risk posture. This incorporates the following two key dimensions from RiskRecon's dataset:

ISSUE SEVERITY Detection of security-relevant issues that expose hosts to various threats. We focus on findings that are rated high or critical according to RiskRecon's categorization.

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.

This approach is consistently reinforced by our research with RiskRecon. For example, our investigation of Internet of Things (IoT) devices from 2020, found a jump of 70 times concerning critical security issues in high-value assets between organizations that expose vulnerable IoT devices to the internet when compared with those that do not. Those organizations that cannot manage the critical security issues affecting their most valuable assets are almost certainly struggling with many other aspects of managing their cyber risk posture as well.

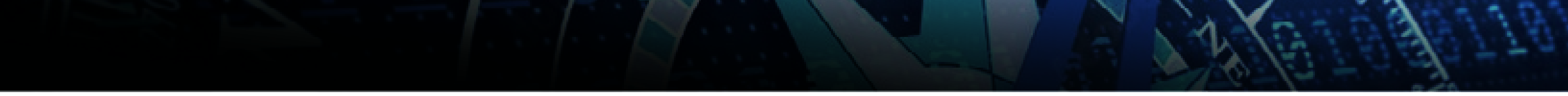


Figure 2 reveals the overall percent of findings that fall in each segment of the risk prioritization of RiskRecon, by comparing the severity of an issue with the importance of the asset on which it exists. Overall, there are relatively fewer findings when we look at the upper right, which are our high-value assets with critical issues. Organizations seem to be doing a pretty decent job at prioritizing the riskiest findings overall. However, we don't deal with "overall" in 3rd party risk management. We deal with specific organizations and their specific risks.

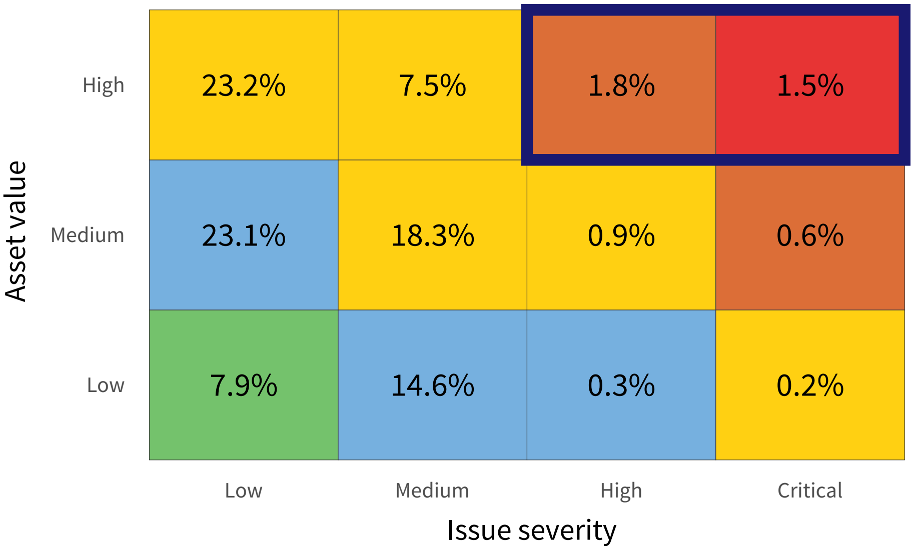


FIGURE 2: DISTRIBUTION OF NON-INFORMATIONAL SECURITY ISSUES ACROSS RISKRECON'S RISK PRIORITIZATION MATRIX

Given that we are defining top performers as organizations that have zero findings and a RiskRecon score of A, and we have identified bottom performers as organizations with the most amount of high-risk finding density, we can take a quick look at Figure 3 to see the results of this categorization.

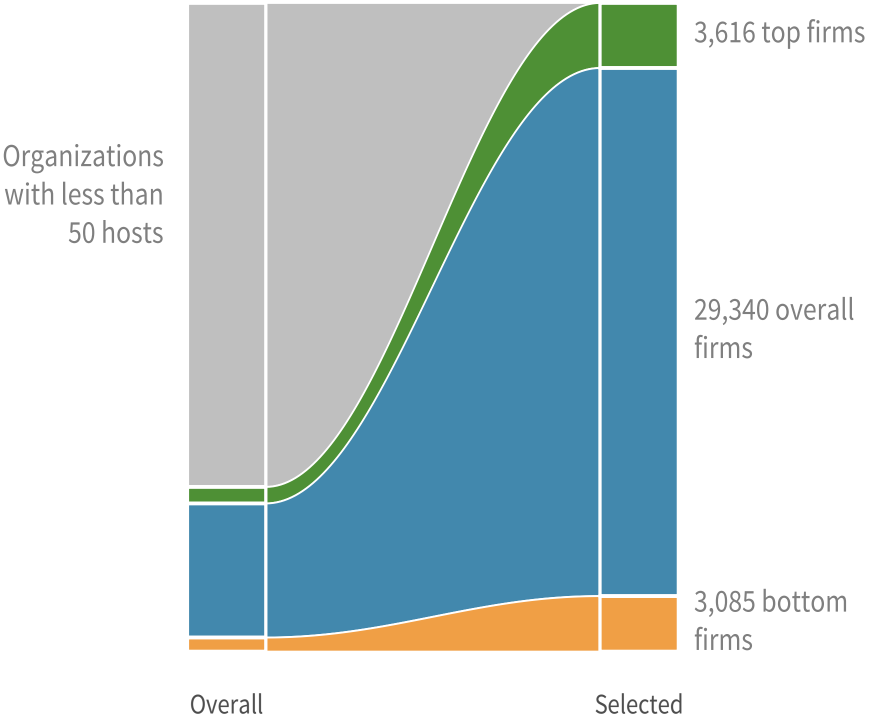


FIGURE 3: COMPARISON OF ORGANIZATIONS IN SCOPE AND PROPORTION OF FIRMS IN EACH CATEGORY

The left column shows the overall scope, with the gray part representing those organizations with less than 50 hosts. The column on the right narrows our focus down to the organizations present within the slices that were focused on and are discussed in this report. While focusing on the endcaps, the overall number will sometimes be used as a point of comparison.

However, the question remains, do we see an obvious difference among organizations when it comes to the Risk Prioritization Matrix?

Let's take a look at Figure 4.

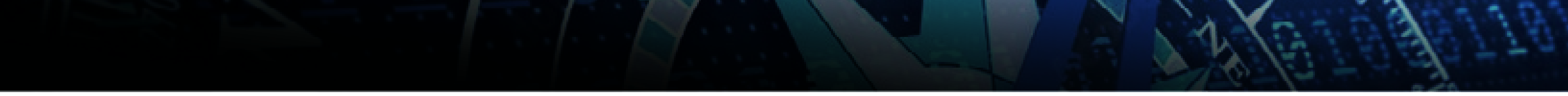
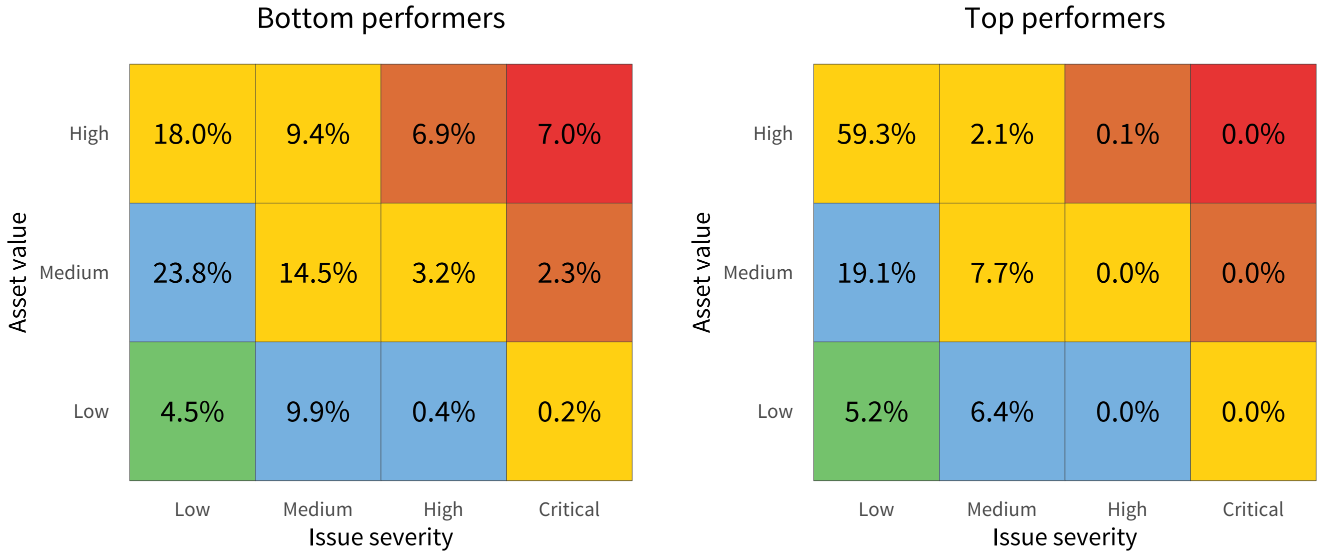


FIGURE 4: COMPARING THE RISK MATRICES OF TOP AND BOTTOM PERFORMERS



Bottom performers

Asset value \ Issue severity	Low	Medium	High	Critical
High	18.0%	9.4%	6.9%	7.0%
Medium	23.8%	14.5%	3.2%	2.3%
Low	4.5%	9.9%	0.4%	0.2%

Top performers

Asset value \ Issue severity	Low	Medium	High	Critical
High	59.3%	2.1%	0.1%	0.0%
Medium	19.1%	7.7%	0.0%	0.0%
Low	5.2%	6.4%	0.0%	0.0%

BOTTOM PREFORMERS

If your organization partners with a bottom performer, and the business relationship involves your data being stored, processed, or otherwise reliant on these systems, then you have cause for concern.

In Figure 4, the left Risk Prioritization Matrix shows the state of issues across the bottom-performing organizations. Looking back at the first version of this matrix in Figure 2, it's clear that these organizations have a higher-than-normal proportion of findings in the high, critical, and generally risky upper-right area of the matrix.

The fact that they have more critical findings on high-value assets than low-severity issues on low-value assets is concerning. If your organization partners with a bottom performer and the business relationship involves your data being stored, processed, or otherwise reliant on these systems, then you have cause for concern.

Conversely, on the right side of Figure 4, the top performers appear to be doing a substantially better job at minimizing high-risk issues, with 0% in the high-value and high-severity corner. Gold star!

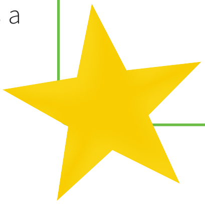
Although security isn't the only decision criterion that you should be focused on when selecting third-party providers, it is an important one. From these matrices alone, there is a strong case for favoring a top-tier partner over a bottom one.

So, can we get to the root of exactly what it is that makes a bottom performer act differently from a top performer?

TOP PERFORMERS

Conversely, the top performers appear to be doing a substantially better job at minimizing high-risk issues, with 0% in the high-value and high-severity corner.

LET'S DIVE IN.



KEY PERFORMANCE INDICATORS

When we think about risk, we also have to acknowledge and account for the inherent risk that is posed to your organization before any mitigation controls. The idea of inherent risk centers around the fact that we often use "common sense" risk factors to build a risk profile of a company before even undertaking any assessment. For example, if you are working with a partner that holds critical information, you may find yourself placing them toward the top of your inherent risk ranking, and pledging to keep a close eye on them.

Throughout this report, we'll put our inherent risk bias to the test and consider some measurable aspects that might influence an organization's risk posture. Why? Because when we look at the measurable things about an organization's risk posture, the same can be used to check for a correlation between the key performance indicators and risk surface.

INDUSTRY CLASSIFICATION

When assessing the risk of third parties, industry is often considered a major driver of risk posture. Research in the past shows that making those assumptions isn't necessarily the most effective thing to do on this front and that the reality is much more complex.

However, while all industries have findings, some have substantially more than others. In order to take a closer look, we present Figure 5 which looks at the spread of findings across firms in different industries. This chart shows that while the median (typical) number of findings often does not vary hugely between the best and the worst groups within an industry, there is a huge variation in the overall number of findings found in firms.

CHOOSE...WISELY

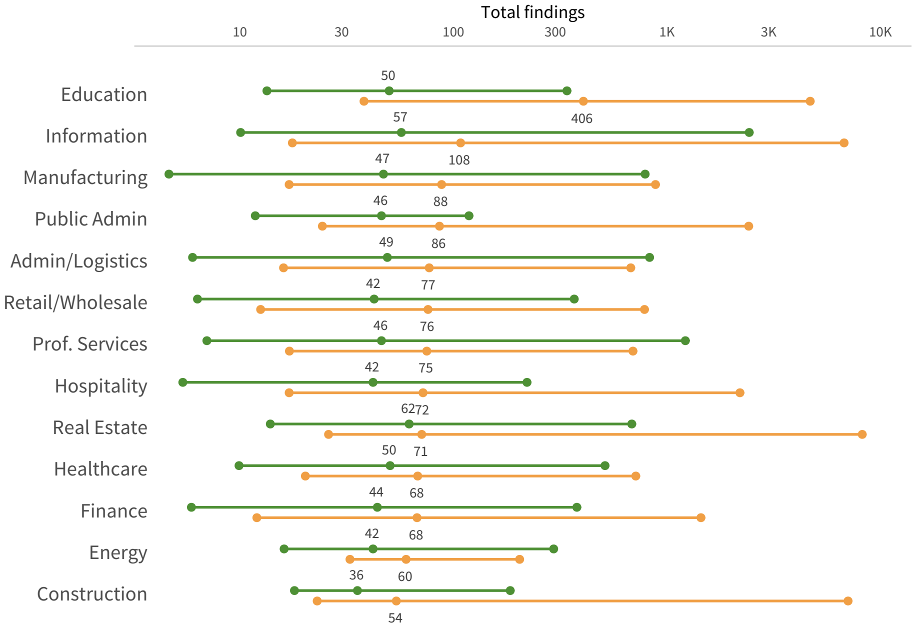


FIGURE 5: NUMBER OF FINDINGS FOUND IN FIRMS ACROSS INDUSTRIES

Education's most challenged organizations have, at the low 5% level, just 38 findings. Whereas, at the 95% level of this same segment, there are 4,685 findings. Real Estate has an even larger range that starts at 26 and goes to 8,212 findings between the two extremes in the bottom performers.

This variance is also seen in the top performer category.

So, while top performers seem to be better at managing their risks across the board, you cannot make assumptions based on industry alone.

Those looking for evidence to support assumption-based claims such as "universities always have poorer security than banks" won't find them here. Instead, we see that the best performers in education are better than the worst performers in finance. Sure, the education sector as a whole may have the highest (read: worst) median density of high findings, while finance may appear much better on the list. However, there is a large amount of overlap between the two.

What does this mean? That there is far more variation within industries than between them. This is important because, typically, third-party risk decisions are made relative to a particular type of organization within an industry. The best partner in education might still manage risk better than the worst partner in finance. When you partner with a top-performing firm, you are more likely to have fewer findings, regardless of industry.

This tension between the number of findings and the amount of variability within industries is presented in Figure 6. Looking at the finding density across industries, we can see how much key industries such as construction and education stand out from the rest of the pack.

WHEN YOUR PARTNERS HAVE MORE FINDINGS, AND MORE VARIABILITY IN THEIR FINDINGS, YOU MAY FIND YOURSELF IN A POSITION WHERE YOU ARE TAKING ON MORE RISK THAN YOU MAY WANT.

We've divided it into four quadrants - less exposed and more variable, less exposed and more consistent, more exposed and more variable, and more exposed and more consistent. While construction is more exposed to risk, it is also consistently more variable, whereas education, while consistent, has a much larger risk exposure. When your partners have more findings and more variability in their findings, you may find yourself in a position where you are taking on more risk than you may want.

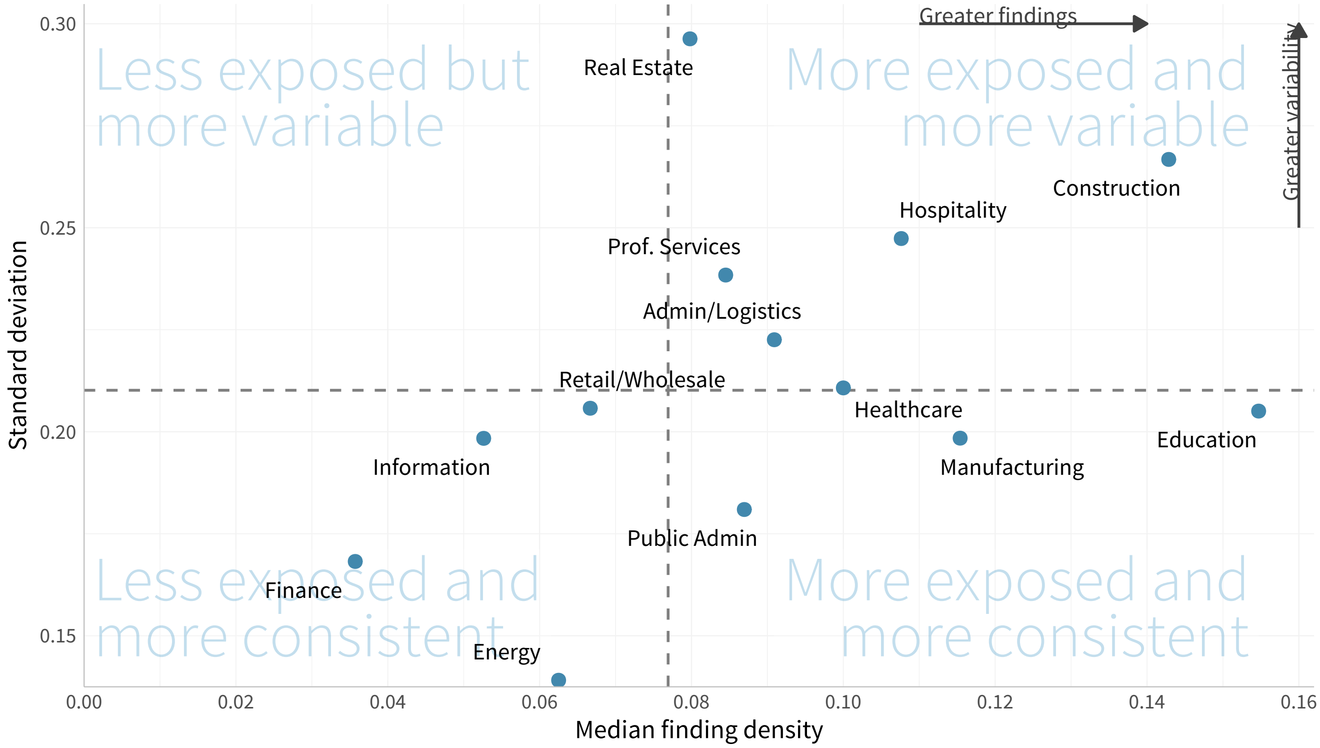
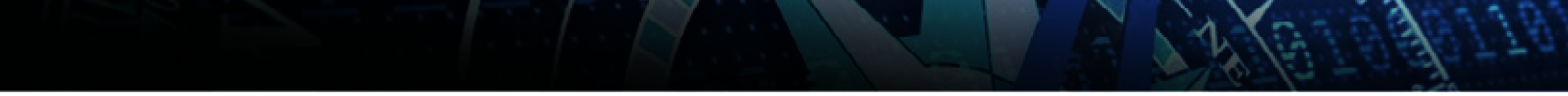


FIGURE 6: COMPARING INDUSTRIES BY MEDIAN FINDING DENSITY AND VARIABILITY

Figure 7 below expands on this trend with a little more detail - because who doesn't love a ranking chart? When we look along the industry slices, we see that one in four businesses in the top performers ranking is either Information or Finance.



However, following Information over to the bottom performers' column, we also find that it is ranked 2nd among the bottom performers. When we follow Finance, we have a bigger drop-off when we look at the bottom performers' column, and the data tells us that one in 11 of the bottom performers is in Finance, i.e., a -162.8% change. This reinforces that, on the whole, Information and Finance industries generally have strong security practices. However, you cannot blindly apply that across the board to include ALL Information industry partners, since the Information industry also holds the silver medal amongst the bottom performers.

Education, on the other hand, has a large increase – 247% – in prevalence among the bottom performers. While 1 in 49 firms in the top performers is from the Education sector, Education makes up 1 out of every 14 of the bottom performers.

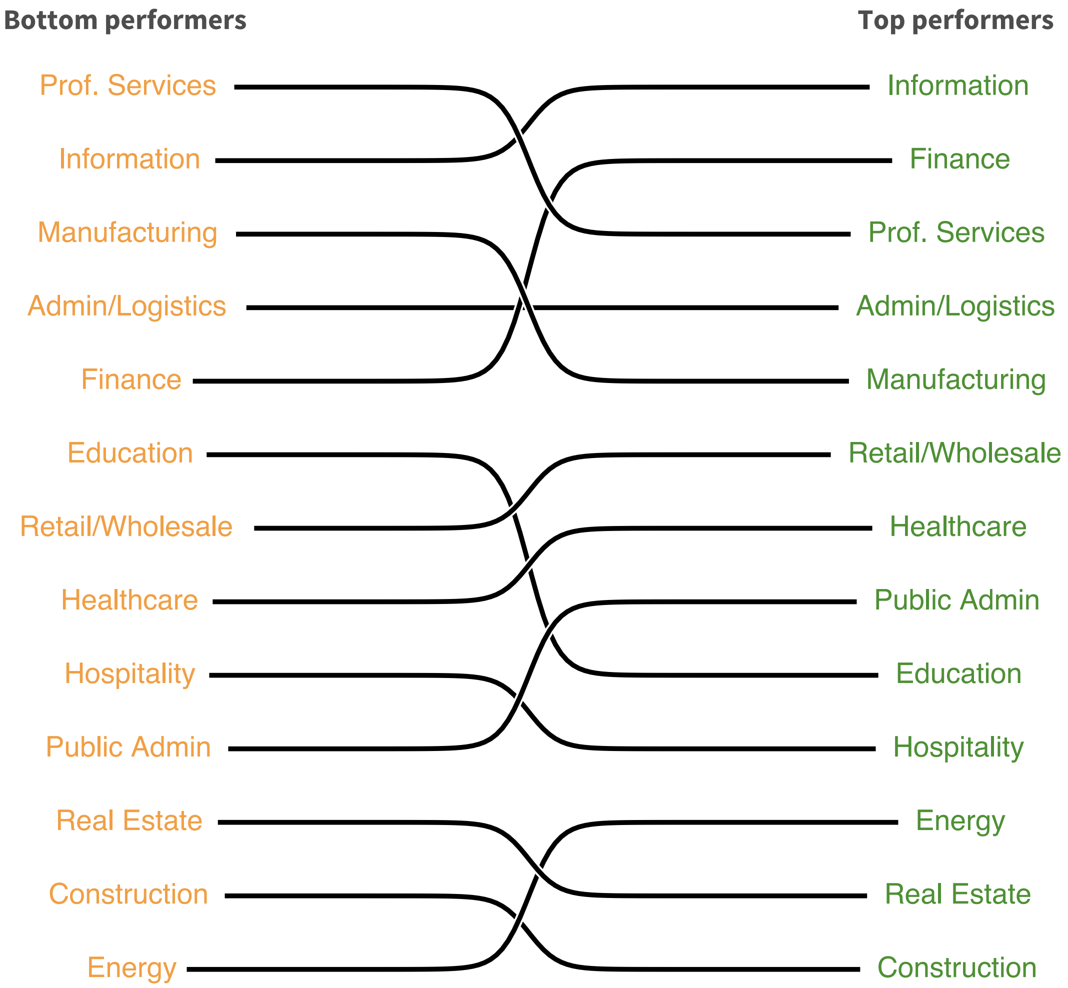
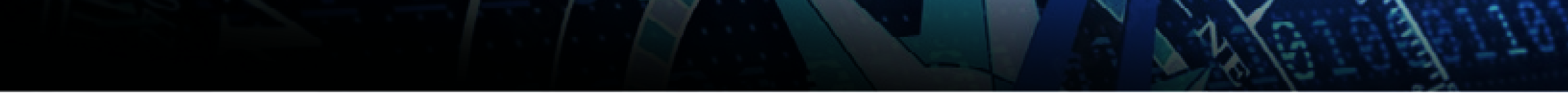


FIGURE 7: INDUSTRY PREVALENCE IN BOTTOM AND TOP CATEGORIES

This could be due to various reasons such as a varying onboarding time for new technologies and risk mitigation strategies, a larger industry population, or a wider number of technologies that are in play within the industry. This clearly illustrates the vast range of variability within the industry.

Before we wrap up our look at industry, let's take a moment to look at Figure 8 to see what impact that choosing a bottom provider might have on your business.Just by taking a quick look, you can see the immediate impact. When you choose a bottom provider in Education, you are likely to have 43 times the amount of critical findings than when you partner with a top performer.



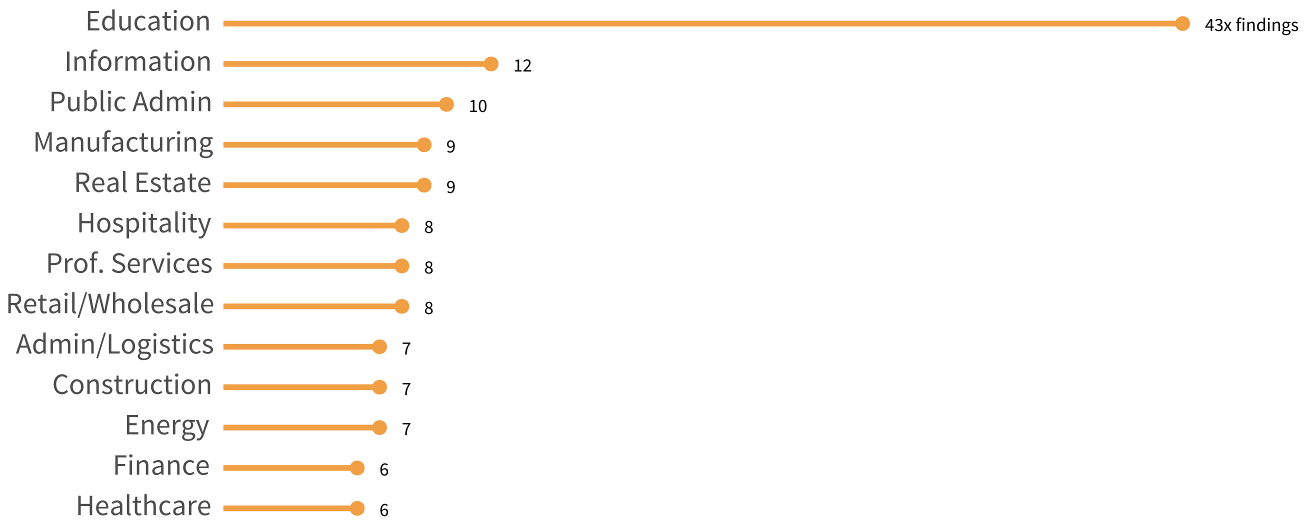


FIGURE 8: PER INDUSTRY DIFFERENCE IN KEY FINDINGS WHEN CHOOSING A BOTTOM VS. TOP PERFORMER

It's clear that your partnering decisions do matter, but industry isn't the end-all and be-all consideration. If you are a risk manager who is looking for a new partner, you'll need to look beyond the industry before making your decision.

ASSET COUNT AND VALUE

Aside from the industry, the number of assets a company has, and how valuable they are, is another factor that's often used to rank and stack third parties based on perceived risk. It's also worth noting that there are differences of opinion on this. Is it easier to keep a smaller digital footprint tidy or is it that the higher budgets and resources of larger enterprises give them an advantage?

Buried in the mass of points on the top of Figure 9 is a slight negative relationship between the number of internet-facing hosts and the density of high-risk findings.

This implies that more hosts seem to correlate with lower density, which makes sense: security issues become less saturated as the digital footprint grows.

The chart on the bottom interjects a "yes, but" into the conversation. It shows that more hosts generally equate to more security issues overall. No shock there but this definitely is something to keep in mind.

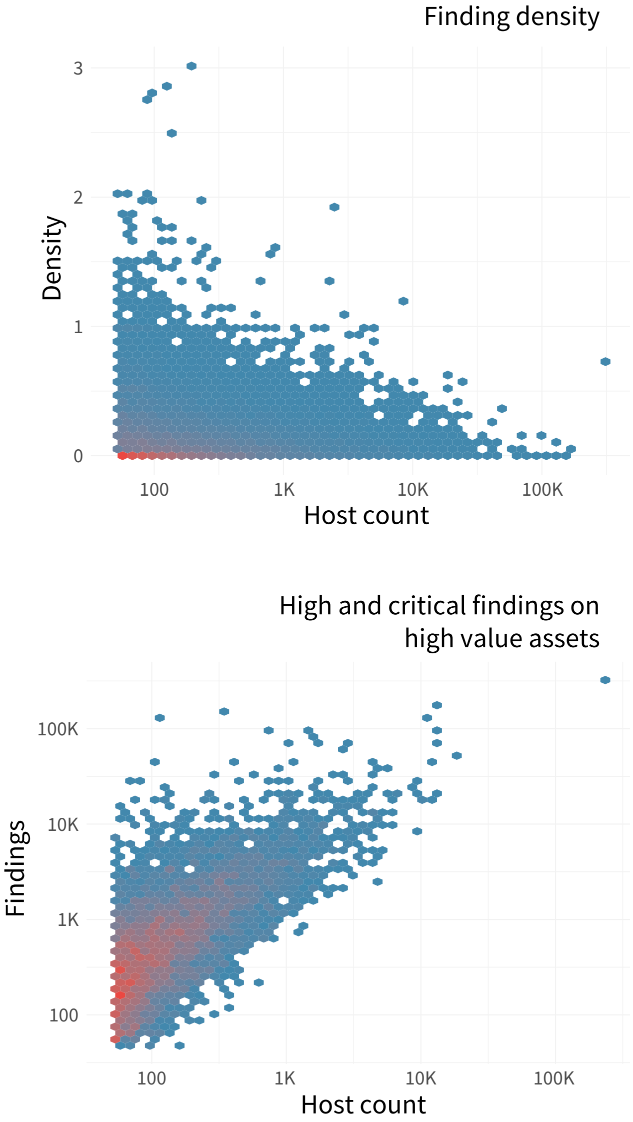


FIGURE 9: COMPARING FINDING DENSITY AND TOTAL KEY FINDINGS AGAINST THE NUMBER OF HOST

Before answering the question that started this section, let's take a quick look at Figure 10. It offers an interesting view of industries based on their median density of findings and the median number of assets. The first thing we notice is the stereotypical separation between the sectors, Education and Finance. In the upper-right, educational institutions struggle to minimize security issues across a sprawling digital footprint. Whereas, financial institutions, with their regulation-motivated tight grip on assets, land (on average) on the opposite side.

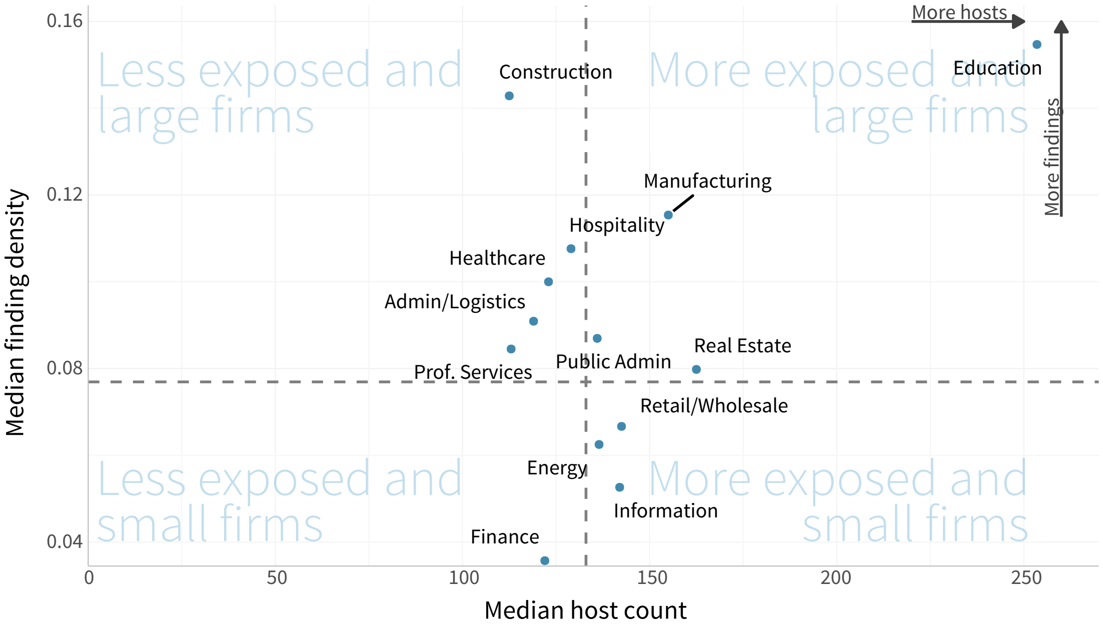


FIGURE 10: INDUSTRY-LEVEL MEDIAN FINDING DENSITY COMPARED TO MEDIAN NUMBER OF HOSTS

Now, back to the question at hand: Can we use the number of digital assets under management as a quick way to risk-rank organizations? Figure 11 answers this with a resounding "nope." The top- and bottom-performing organizations have a nearly identical distribution of active hosts. And to be honest, that is surprising, especially in light of Figure 8.

We love it when data surprises and corrects our intuition and implicit bias, which sometimes lead to uninformed decisions.

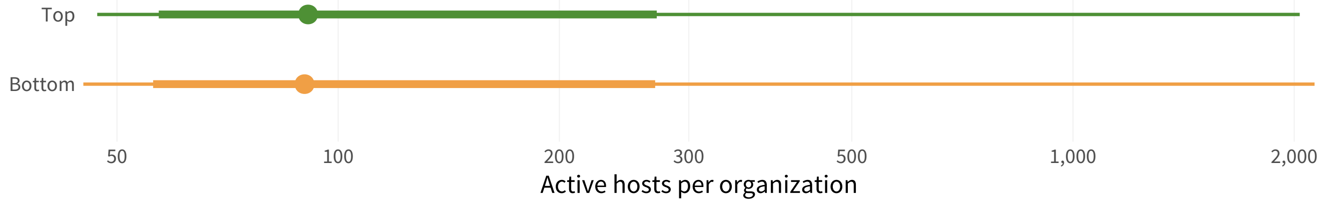


FIGURE 11: COMPARING TYPICAL ACTIVE HOSTS ACROSS TOP AND BOTTOM PERFORMERS

Let's check one more risk surface dimension before leaving this section: asset value. If the raw number of hosts cannot differentiate between the top and bottom performers, then perhaps having a high proportion of assets that collect sensitive information, authenticate users, and run critical services might do the trick[2].

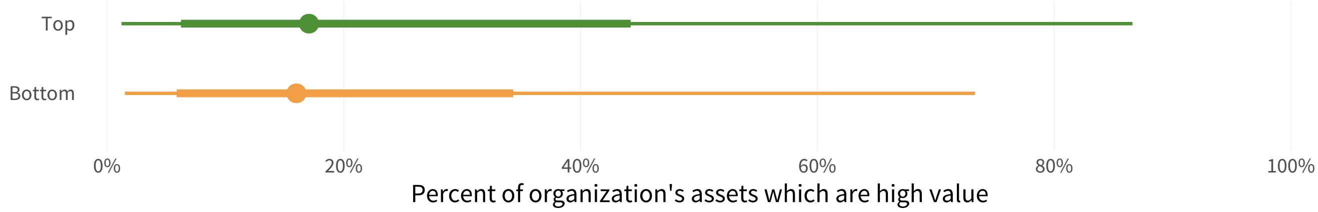


FIGURE 12: HIGH VALUE HOST CONCENTRATION AMONGST TOP AND BOTTOM PERFORMERS.

[2] Assets determined to have such functionalities are classified as high-value by RiskRecon.

What is interesting here is that the proportion of high-value hosts does not seem to be a clear separator of the top and bottom performers. Not only is there an incredible amount of overlap, but the median is also nearly the same. As with host count, there is almost no discernible way to conclude that having more or less high-value hosts automatically makes an organization a top or bottom performer.

GEOGRAPHIC DISTRIBUTION OF HOSTS

The internet is often described as borderless, so it might seem a little odd to take a look at where the hosts are located. Although the virtual and physical worlds differ in many ways, different parts of the world have different policies, regulations, and customs that govern the hosts and data. Organizations with larger geographic footprints must manage a larger portfolio of geopolitical, legal, compliance, and physical risks tied to those geographies. As an indicator of such complexities, we examine the proportion of hosts located within and outside of a firm's home country of operation.

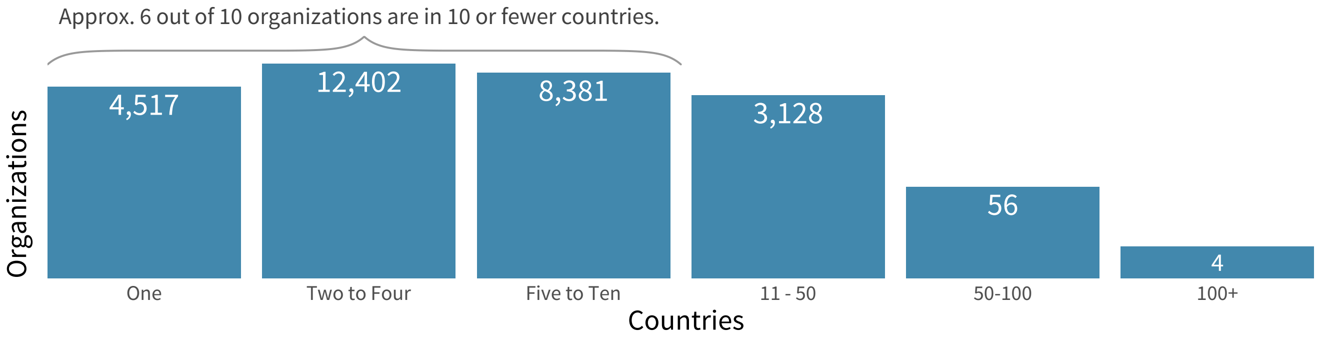
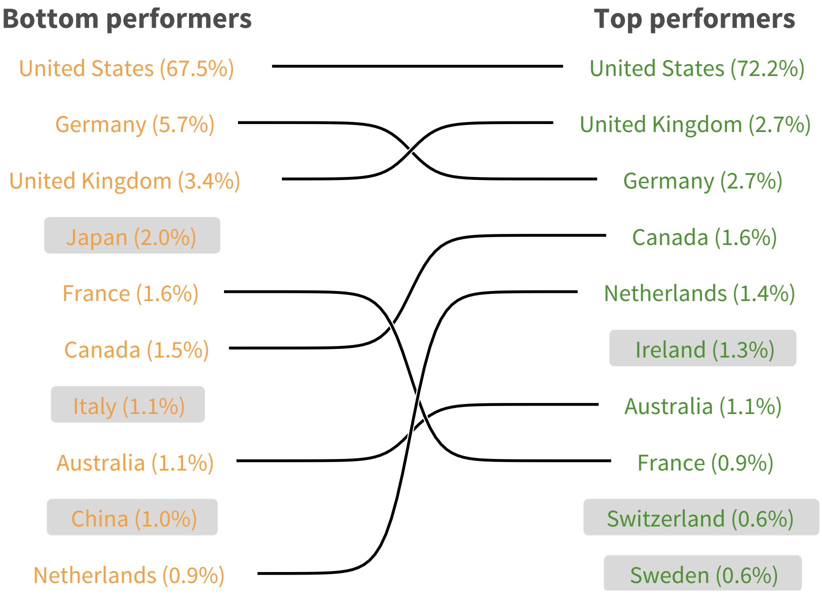


FIGURE 13: NUMBER OF COUNTRIES IN WHICH ORGANIZATIONS OPERATE



We see that approximately six out of 10 organizations have their hosts in 10 or fewer countries. This could simply be due to the size of the organization. However, whether a potential partner has hosts strewn across the globe or consolidated in a single country, the number of countries the hosts are located in doesn't seem to be an indicator of their security posture.

So, let's dive a little deeper and look at the individual host country levels of high-value hosts against the top and bottom performers.

FIGURE 14: HOST COUNTRIES WITH TOP PERFORMERS VS. BOTTOM PERFORMERS

To clarify, when talking about host countries, we are looking at the primary country where the majority of a firm's assets are located. The top three host countries are virtually the same for both top and bottom performers. 72.2% of top performers primarily have hosts within the United States, and 67.5% of bottom performers have hosts within the United States. We can also see that Germany makes up 2.7% of the top performers, but 5.7% of the bottom performers. France nearly doubles its relative ranking, from 0.9 at the top to 1.6% at the bottom.

What you might notice here is that there are certain countries that do not show up on both the lists. Ireland, Switzerland, and Sweden are only represented in the top performers' list. Whereas, Japan, Italy, and China are only represented in the bottom performers' list.

So what does this actually mean? Are certain countries more or less secure than others? It looks like this can be answered with a "maybe." Since the majority of top and bottom performers have hosts located within the United States, United Kingdom, and Germany, it's hard to say. However, the fact that certain countries only show up on the bottom performers' list may have to do more with the organization and upkeep of the hosts and assets than the hosts' geographic location.

So, if geographic locations do not necessarily show a difference, then let's look (up) at the next possible host location: the cloud.

CLOUD, WITH A CHANCE OF FINDINGS

So, let's first take a look at how organizations are adopting the cloud. Right off the bat, we notice that many industries are just about to, or very close to, shifting majority cloud, which is an amazing shift in the balance of host locations over the years. We can also see that the industry bookends of Education and Real Estate, which shows how cloud readiness, along with their adoption rates, may start to create a clearer picture of what differentiates a top and bottom performer. Again, this is not to say that the best in Education are not doing better than worst in Real Estate.

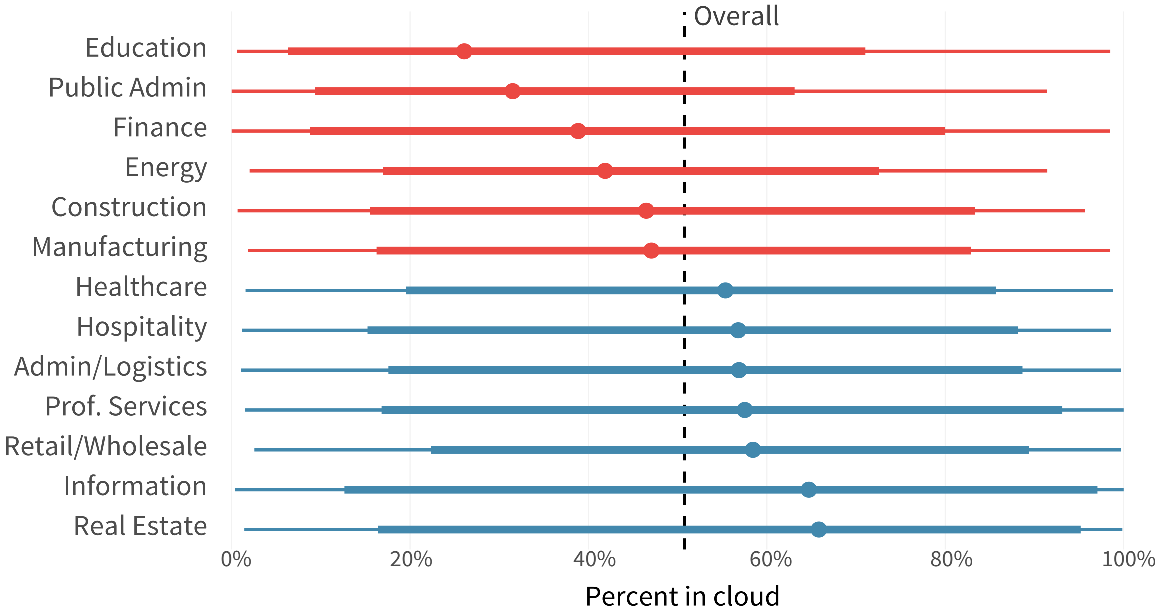
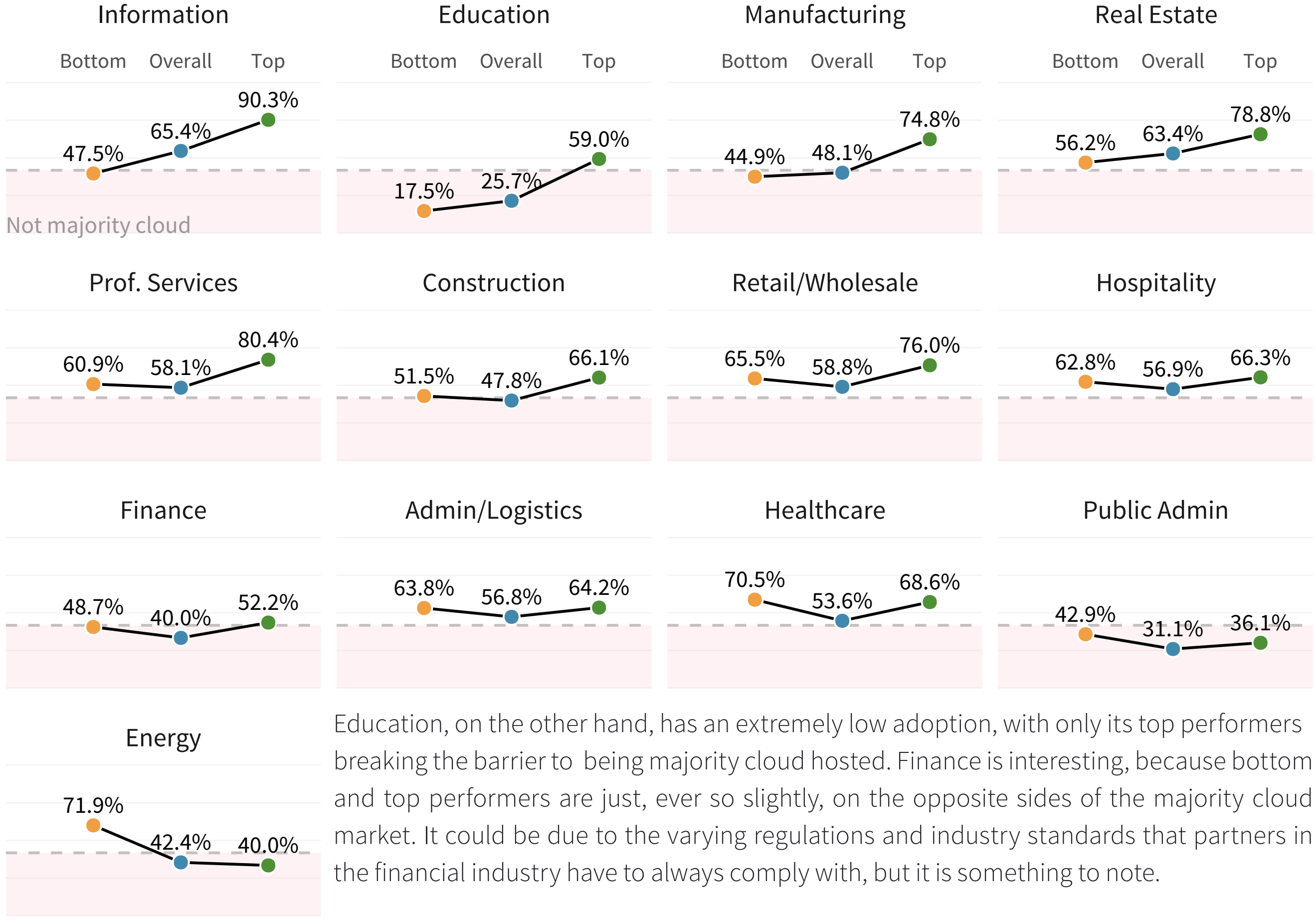


FIGURE 15: INDUSTRY-LEVEL CLOUD ADOPTION

Figure 16 shows the drastic variation in cloud adoption per industry. For example, it's no surprise that the Information industry would be a majority cloud industry, with 90% of its top performers choosing to use the cloud to host their assets.

FIGURE 16: INDUSTRY CLOUD ADOPTION, SEPARATED BY TOP AND BOTTOM PERFORMERS



Education, on the other hand, has an extremely low adoption, with only its top performers breaking the barrier to being majority cloud hosted. Finance is interesting, because bottom and top performers are just, ever so slightly, on the opposite sides of the majority cloud market. It could be due to the varying regulations and industry standards that partners in the financial industry have to always comply with, but it is something to note.

Information seems to be the clear leader in cloud adoption, which highlights how far behind the rest of the industries are when it comes to shifting toward cloud partners.

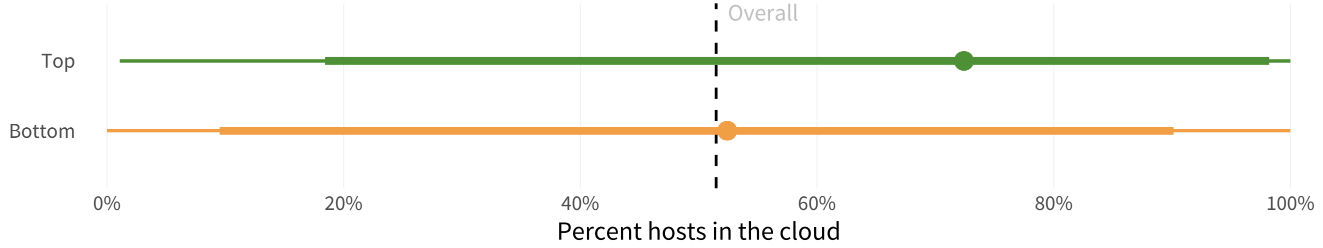


FIGURE 17: TOP AND BOTTOM CLOUD ADOPTION RATES

When we take a look at the cloud adoption rates of the top and bottom performers, we start to see some very clear separation. There is a clear gap between the top and bottom performers when we look at Figure 16. Every 10% increase in host cloud concentration, results in a 2.5% increase in the probability of being a top performer.

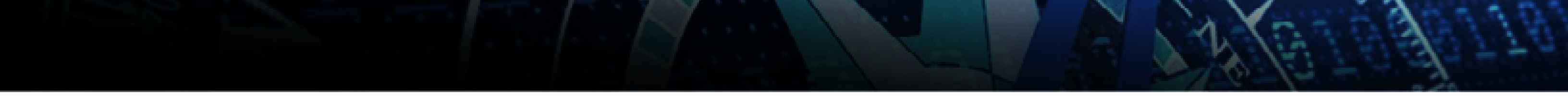
We can now clearly see that the top performers are more likely to have hosts in the cloud. However, what difference does it make if the best of the bottom performers are still better than the worst of the top performers?

It makes a BIG difference.

EACH 10% INCREASE IN CLOUD CONCENTRATION RESULTS IN

2.5%

INCREASE IN BEING A TOP PERFORMER



FIRMS THAT ARE CLOUD FIRST WITH A SINGLE PROVIDER RESULTS IN

84.8%

Cl 74.8% - 94.9%

INCREASE IN BEING A TOP PERFORMER

First off, we can see that choosing a cloud is way less important than deciding to go cloud-first.

The data tells a big story, because when an organization decides to be cloud-first with a single provider they have, on average, a nearly 85% higher chance of being a top performer. So, does who you choose to go with matter? Choosing to go majority cloud with one of the 'big three' cloud providers, namely AWS, Azure, or GCP, has inconsequential effects rather than being simply cloud-first. Being in the 'big three' of cloud providers may have other advantages; however, moving to a cloud-first approach has the largest impact on whether a partner can be considered a top or bottom performer.

So, if the cloud has such a big impact on determining whether a partner is a top or bottom performer, then does the tech footprint of an organization also have an impact?

TECH FOOTPRINT

When we talk about the technological footprint of an organization, we are referring to how many different technologies are in use. We'll dive into the specific technologies later on, but let's take a look at whether the sheer number of technologies used influences what makes a top or bottom performer.

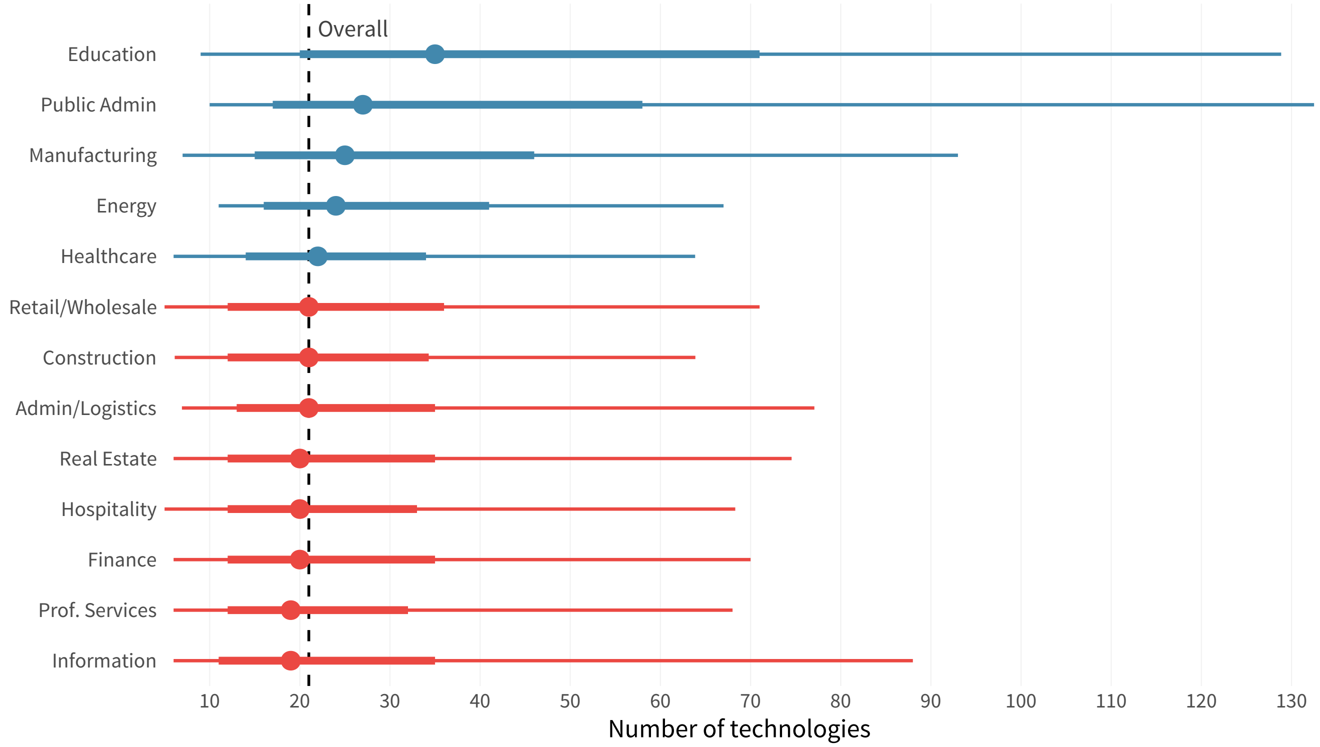
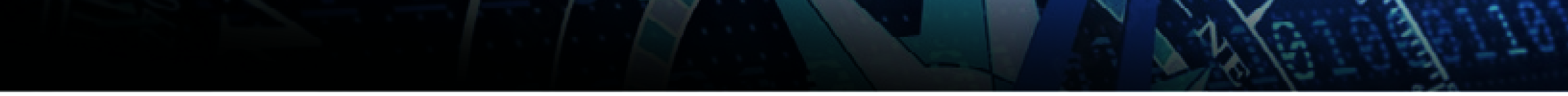


FIGURE 18: NUMBER OF TECHNOLOGIES EMPLOYED ACROSS INDUSTRIES

Education sits high on the list, with the most number of technologies in play, which is no surprise, while Finance, Professional Services, and Information are at the bottom. Industries like Finance rely heavily on regulated technologies, processes, and compliance standards to help minimize their risk. So, it comes as no surprise that industries that have a lot of regulation around them would have a smaller technical footprint. Seeing Energy and Manufacturing high up may, at first glance, be surprising. However, they have a very wide breadth of organization types and verticals within them, which may account for the range in the technical footprint size.



	Admin/Logistics	Construction	Education	Energy	Finance	Healthcare	Hospitality	Information	Manufacturing	Prof. Services	Public Admin	Real Estate	Retail/Wholesale
jQuery	98.7%	96.6%	99.5%	99.7%	98.3%	98.1%	96.8%	98.3%	98.5%	98.2%	99.1%	98.7%	96.7%
Apache	83.5%	84.0%	90.8%	92.2%	85.3%	87.2%	84.4%	74.1%	88.4%	78.3%	89.4%	79.2%	85.9%
Twitter Bootstrap	85.0%	82.0%	95.2%	92.2%	86.1%	85.8%	80.3%	83.2%	87.1%	81.8%	95.7%	84.4%	83.3%
ASP.NET	81.7%	87.9%	90.9%	94.6%	82.3%	89.1%	79.5%	63.8%	86.5%	73.2%	92.9%	81.0%	81.0%
Google Analytics	82.2%	79.1%	93.2%	82.0%	79.0%	81.6%	78.9%	81.1%	83.6%	78.4%	90.2%	83.4%	80.3%
Nginx	81.3%	71.4%	92.1%	79.3%	78.8%	78.4%	85.1%	85.7%	84.5%	80.6%	78.4%	74.4%	83.4%
Microsoft IIS	78.0%	82.5%	89.8%	93.1%	79.7%	85.8%	73.6%	60.1%	82.4%	69.7%	93.4%	75.7%	76.4%
YouTube	77.1%	70.9%	92.2%	80.5%	69.1%	84.2%	71.4%	71.8%	78.8%	71.0%	90.4%	76.3%	71.6%
Google Tag Manager	76.2%	62.6%	84.4%	75.7%	76.1%	82.2%	83.6%	75.0%	78.6%	70.2%	65.9%	74.4%	78.2%
WordPress	63.0%	67.0%	78.9%	61.3%	52.7%	67.5%	63.4%	59.7%	67.0%	62.6%	65.9%	68.3%	55.9%
Windows Server 2016	62.6%	70.9%	82.1%	82.3%	63.1%	67.5%	58.0%	48.8%	68.4%	56.5%	85.2%	60.9%	59.4%
Modernizr	61.5%	56.3%	83.1%	70.6%	60.5%	63.1%	64.1%	52.7%	66.0%	53.1%	76.6%	61.2%	57.3%
Windows Server 2012 R2	56.4%	60.2%	76.7%	71.5%	57.7%	70.7%	48.6%	39.4%	61.9%	49.2%	83.6%	53.0%	54.3%
libssh	56.7%	63.1%	74.9%	57.7%	48.6%	53.1%	56.8%	57.2%	69.0%	56.2%	60.2%	54.6%	55.2%
OpenSSH	51.5%	53.9%	70.7%	53.5%	42.3%	54.5%	52.9%	45.5%	61.7%	48.1%	59.1%	53.6%	47.9%
Microsoft HTTPAPI 2.0	45.6%	53.4%	65.2%	63.4%	47.1%	56.4%	36.7%	33.6%	54.4%	40.8%	70.7%	42.7%	45.5%
PHP	38.4%	42.7%	65.7%	39.3%	34.4%	36.3%	39.4%	37.2%	49.1%	36.1%	49.5%	40.9%	37.1%
Ubuntu	36.1%	30.1%	65.3%	32.1%	29.5%	30.1%	38.5%	42.1%	45.0%	37.6%	42.7%	35.4%	39.1%
BigIP	25.6%	21.4%	35.7%	48.9%	43.1%	28.8%	20.7%	18.6%	28.0%	17.3%	44.1%	24.0%	30.1%
Varnish	29.2%	16.0%	49.6%	24.6%	22.7%	26.0%	28.0%	34.6%	30.5%	26.1%	37.0%	27.7%	28.1%
CentOS	23.0%	20.4%	56.0%	24.3%	19.7%	18.4%	25.1%	27.5%	30.1%	24.9%	30.7%	29.0%	25.0%
Drupal	22.6%	14.1%	49.1%	29.7%	22.4%	26.0%	19.2%	16.9%	25.4%	15.3%	43.4%	16.6%	14.5%
Express	20.5%	16.0%	37.6%	19.8%	21.8%	12.1%	21.6%	30.7%	23.6%	21.4%	29.8%	19.0%	24.0%
OpenSSL	0.1%	0.5%	0.9%	0.3%	0.1%			0.1%	0.1%	0.0%	0.4%		0.2%

FIGURE 19: CONCENTRATION OF TOP 25 TECHNOLOGIES ACROSS INDUSTRIES

The top-25 technologies per industry are pretty impressive, with jQuery heavily favored across the board. However, we can see some variation in use. For instance, PHP's largest presence is in Manufacturing and Information, while Ubuntu is being used primarily in Education. Apache is still being used heavily across the board, i.e., between 74.1 and 90.8%, across all industries. OpenSSL, on the other hand, shows up as less than a percentage across the board.

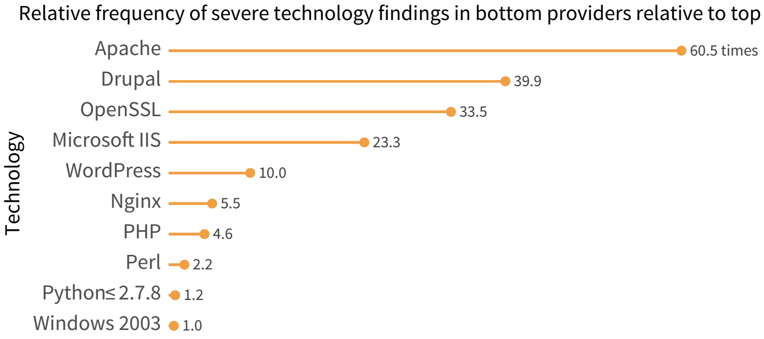


FIGURE 20: COMPARING THE TOP PROBLEMATIC TECHNOLOGIES OF BOTTOM PERFORMERS TO THOSE SAME TECHNOLOGIES IN TOP PERFORMERS

Just because an organization has a bigger technological footprint, it doesn't necessarily mean that it's a more problematic footprint. So, we took a look at the top problematic technologies of bottom performers.

While looking at the percentage of severe instances against certain problematic technologies, findings around Apache are 60.5 times more frequent in bottom performers than they are in top performers. Drupal and OpenSSL round out the top three technologies that carry severe technological findings in bottom performers.

SO, WHAT DOES THIS MEAN?

THIS MEANS THAT WHEN YOU ARE EVALUATING A POTENTIAL PARTNER ORGANIZATION, TAKE THE TIME TO LEARN MORE ABOUT THEIR TECHNOLOGICAL FOOTPRINT AND THE KIND OF TECHNOLOGIES THEY USE. TAKING THE OPPORTUNITY TO CHAT ABOUT PATCHING PROCESSES OR CYBER HYGIENE PRACTICES CAN HELP YOU MAKE A BETTER-INFORMED RISK-POSTURE ASSESSMENT.

FINDINGS

We've taken a look at a lot that tells us how each organization's risk surface is dependent on the choices that it makes, regardless of the industry. Many of these factors such as the number of hosts and geographic location have little effect on separating the winners and losers, while others such as cloud adoption have a significant effect on where an organization lands.

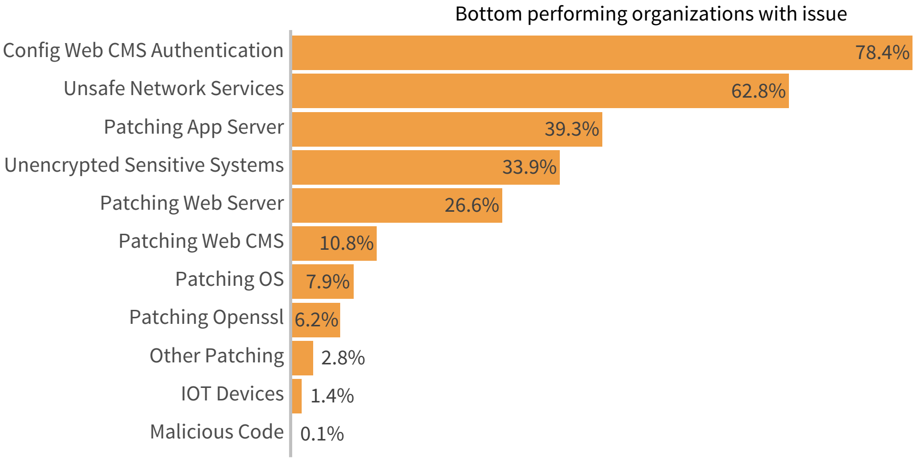


FIGURE 21: MOST COMMON ISSUES AMONG BOTTOM PERFORMERS

Looking at the technical footprints of firms, again, we see some differences between the top and bottom performers.

Overall, web CMS authentication and patching application servers seem to be the "top" problems for all bottom performers. Patching in general seems to be a recurring issue for bottom performers, so perhaps a good question to ask a potential partner is how they manage to patch their software and tools.

When we look at the unsafe services in the above figure, we notice that MySQL has the most instances among the bottom performers, being the only one to pass 1,000 instances out of all these technologies.

So, what does that mean in terms of what the technologies actually do? Figure 22 shows the distribution of purposes of each of these surfaces. For example, out of all of the database listeners, we see that MySQL has the most instances, while IBM and Cassandra have the least.

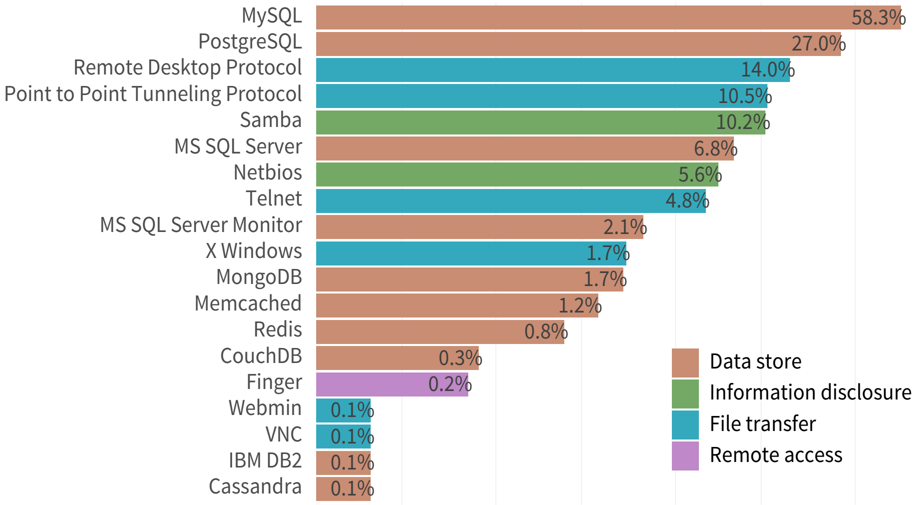


FIGURE 22: UNSAFE SERVICES FOUND IN THE BOTTOM PERFORMERS

When we look at remote access services, the remote desktop protocol has the most instances, while VNC and Webmin have the least. Recognizing that each technology comes with its pros and cons is part of risk management. Further, it is important to be warned that you should take a closer look at the technologies that a potential partner utilizes before making your decision.

There was no time when a top performer had an instance when a bottom performer did not. What this suggests is that it is not necessarily the size of the technical footprint that matters but what technologies make up the footprint.

CONCLUSION

WHAT WE CAN CONFIDENTLY SAY IS THAT WHEN YOU CHOOSE TO PARTNER WITH A TOP PERFORMER, YOU WILL BE BETTER OFF.

HOW MUCH BETTER?

MORE THAN 300-TIMES BETTER.

Assumptions are usually half-based on fact and partly on a mix of urban legends, anecdotes, and educated guesses. When trying to assess the risk surface of an organization, whether it's yours or someone else's, it's tempting to start by making certain assumptions based on the industry the organization is in. What we can confidently say is that when you choose to partner with a top performer, you will be better off. How much better? More than 300-times better.

Such a large multiple must be backed up with data, so we'll add one more chart before closing this report. Figure 23 expands on Figure 1 in the Introduction. It shows the compounding negative impact of choosing multiple third parties from among the bottom performers as opposed to choosing them from among the top performers. There is a clear and large impact on the business decisions we make, and with every incremental increase in the number of firms in your supply chain, the impact of choosing the top or bottom performers will be that much greater.

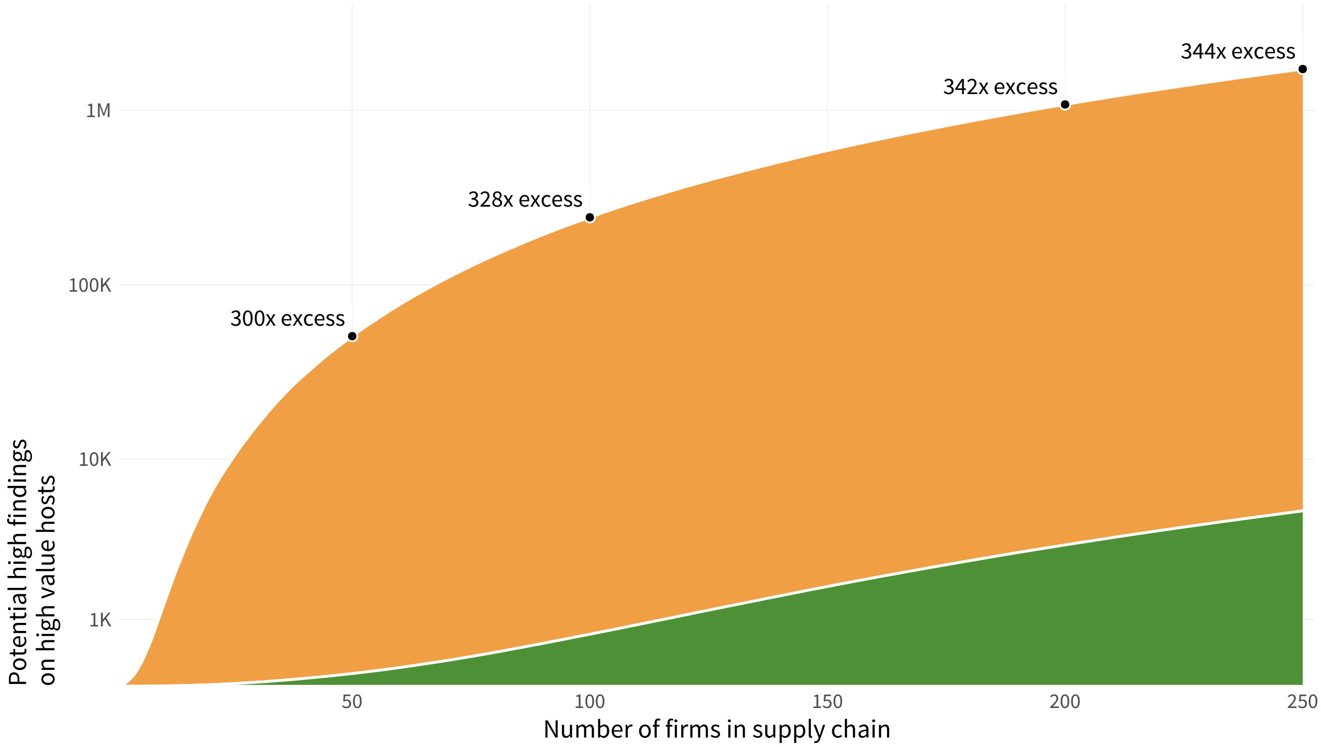
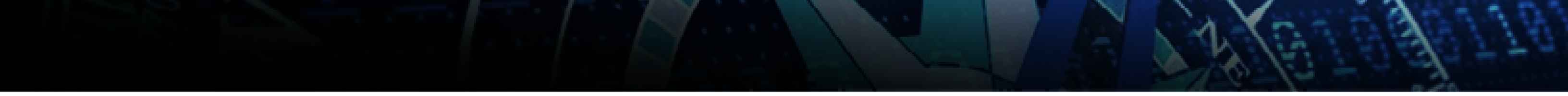


FIGURE 23: CUMULATIVE EFFECT OF CHOOSING BOTTOM OVER TOP PERFORMERS



Whether you are starting to utilize inherent risk rankings or trying to enhance what you currently use for initial vendor prioritization, examining an organization's technical footprint is a component that can greatly impact how you rank your vendors. Take the time to go through the technologies that are being used in addition to taking a look at their technological footprint. How many technologies is this organization not only using but is also responsible for upkeep and monitoring? Are they using a cloud as a host provider? How many severe findings can be found in those specific technologies?

It's these questions, rather than looking at the broader lens of industry, that will help you make the most informed decision around risk. So, while there are several gray zones, and a lot of continuous testing and learning will help you continue to examine yours, and a partners, organization's risk surface and make the best decisions for yourself.

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.

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