REPORT

Under the Surface: Uncovering Cyber Risk in the Global Supply Chain

By Ben Edwards

March 2025

Contents

Introduction

Interconnectedness is a fundamental feature of most human endeavors. Whatever the goal, success regularly depends on the cooperation of different entities, each with their own specialty.

As we have entered the digital age, new specialities and new methods of collaboration have made it easier than ever to work together; software can be installed in minutes, and services can be accessed with a few clicks and keystrokes. This ease of collaboration allows for organizations to focus on their mission, while leveraging others to provide the necessary tools to navigate the rapidly evolving digital landscape. Of course, this extends beyond single relationships. Consumers of one product provide to many others, who themselves provide to many others, and so forth, creating the global supply chain.

However, this interconnectedness is not without risk. By relying on others, organizations develop dependencies over which they may have limited control. This means that disruptions experienced by partners can affect not just a single organization, but also a remarkably large portion of the global economy. Recent history has given us numerous incidents where a disruption at one single company has long-ranging and cascading effects. To name a few in the first half of the current decade:

- **SolarWinds (December 2020)**
- **Colonial Pipeline (May 2021)**
- **Kaseya (July 2021)**
- **PyTorch (December 2022)**
- **TSCM (February 2023)**
- **3CX (April 2023)**
- **Apple, Microsoft, others**
- **Okta (October 2023)**
- **Snowflake (May 2024)**
- **Crowdstrike (July 2024)**

In many of these cases, an unexpected yet critical player in the global supply chain experiences an event (whether because of a targeted attack or an unfortunate circumstance) that causes (or had the potential to cause) cascading effects. Costs for these types of events are difficult to assess, but estimates usually break into the billions of dollars and sometimes orders of magnitude more, with insured losses only covering a fraction of the overall event. In our ever more connected world, in which nearly all interactions are mediated through the internet, having an in-depth knowledge of the digital supply chain, understanding risk, and taking action is critical.

Bitsight believes that the best way for the global market to address these challenges is through the use of principled, data-driven analysis of interconnectedness and exposure. We are in a unique position to offer insights into this increasingly common and impactful problem. This report leverages Bitsight data drawn from a variety of sources, including third-party relationships, our security scanning technologies, entity mapping, and financial data.

Our array of data resources gives us one of the most comprehensive pictures of what the global digital supply chain looks like, where critical links might lie, and the cybersecurity performance challenges that organizations face.

But before we begin to wade through this data, we need to define what exactly a supply chain is and what our data covers. There are numerous definitions, but the National Institute of Standards and Technology has a very good one:

> *Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer. -NIST SP 800-37 Rev. 2*

In this work, we are going to examine the organizations that deliver the resources and processes (**Providers**) and those that consume those resources and processes (**Consumers**). We'll also save some characters and refer to "resources and processes" as **Products**. The above is an expansive definition, and one that we, or indeed anyone, would be able to quantify on a global scale. Moreover, Bitisight, being a cyber risk intelligence company, is most interested in the **digital supply chain**: those products that only operate through the medium transistors that make our modern world tick.

In particular, we examine the digital supply chains of more than 500,000 consumer organizations, using 42,600 different products across 12,000 providers, comprising nearly 61.5M relationships. This allows us to make several key observations:

1. **Supply chains are vast.** We find that a typical organization employs hundreds of products from dozens of providers.
2. **Providers have 2.5x larger supply chains compared with the consumers they serve.** The providers we observe in our data set tend to have larger supply chains compared with their consumer customers. With a larger attack surface to defend, providers tend not to perform as strongly as consumers.
3. **There are several areas of concentrated risk across the supply chain.** In some sectors and industries, providers who serve <1% of companies service more than 50% of the market share (based on their clients' revenue).
4. **We highlight the "Critical 99," the top 99 providers weighted by revenue to determine the proportion of the market share they serve.** Additionally, we analyze "hidden pillars," specialized providers that, despite lacking global reach, play a crucial role in major industries.
5. **33% of US organizations rely on companies listed by the US Department of Defense as "Chinese Military Companies."** In the current geopolitical zeitgeist, it is more important than ever to understand "who" is in your supply chain.

These insights give shape to the complexity that securing the global digital supply chain presents.

How big are Digital Supply Chains?

The first questions to ask before any data-driven investigation of supply chain risk should be “what is it composed of?” and “how big is it?” Of course, enumerating all of the resources and processes used by any organization is challenging, but identifying those relationships is Bitsight’s bread and butter. We do our best to enumerate those products and services and categorize them into a few buckets:

Products. Any product or service that an organization does not provide itself, but rather relies on others. While this can mean either digital or physical products, in this research, most are digital. Even traditionally physical services (say logistics and or shipping) are highly digitized and subject to incidents and outages. We categorize these into different categories of products (more on these below).

Provider. Another organization that provides said products.

Consumer. An organization that consumes a product from a provider.

Internet Facing Digital Assets. Bitsight’s business was built on scanning the entire internet and looking for resources (services running on IPs, websites, and other assets) and assessing their security. Moreover, we are able to associate those resources with particular organizations.

Hosting Providers. Many organizations don’t host their own technical resources. It’s interesting to understand what work they offload on others, and how often they do so. In particular, cloud services providers handle websites, data storage, and computation for consumers.

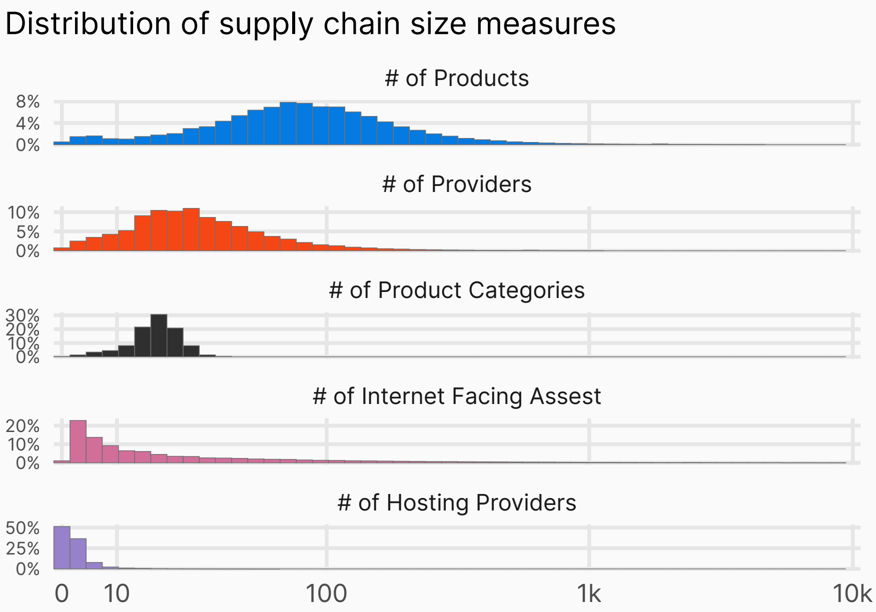


Figure 1 Overall size of supply chain by various measures.

Figure 1 displays the frequency distribution of each of these metrics for a little more than half a million organizations.

The scope of Figure 1 clearly shows that the size of a digital supply chain can be vast. Some organizations rely on thousands (or, in rare cases, tens of thousands) of different products supplied by hundreds of providers. Despite this “heavy tail,” we see that organizations still typically have to manage around 100 different products spread across a dozen or so providers. When each of these providers has their own risk profile, we start to see hints of the complexity of supply chain management from this single chart.

Of course, one of the key ideas behind supply chain risk is that the organizations you depend on also depend on others (and they depend on others and so on), constructing the metaphorical "chain" of dependencies that are needed to keep the global economy afloat.

These chains contain a great deal of complexity, which we'll save for later research. But we do want to pull back the curtain a bit to give you an idea of how that complexity manifests. Suppose we were to take all of the organizations in Figure 1 and then divide them into those that are known to supply digital products and services to other organizations (or that we have data indicating they do), and those that only consume products and services (Figure 2).

Key Point
The typical organization has to manage hundreds of products, and dozens of providers in direct relationships. This does not include the extended "nth party" relationships (the suppliers of suppliers).

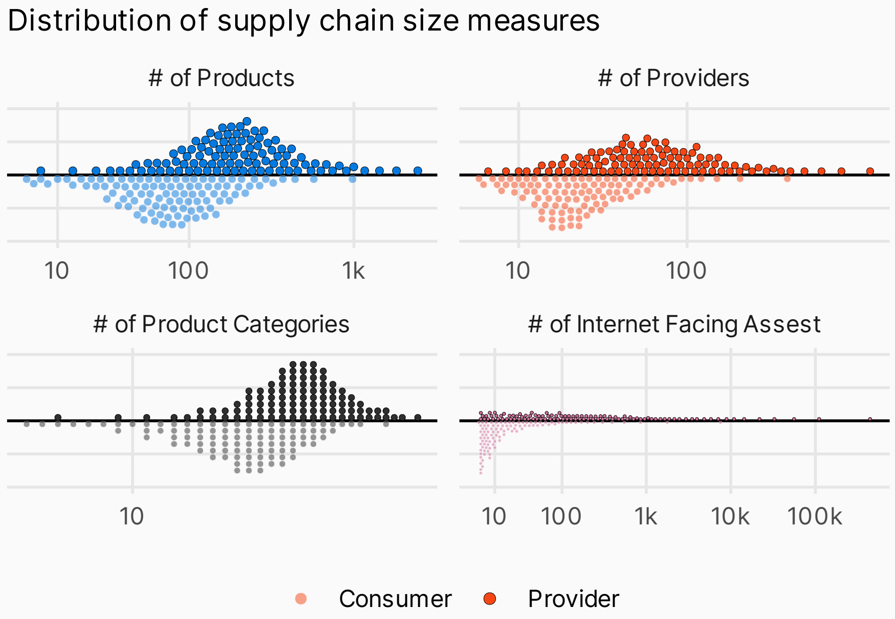


Figure 2 Supply chain size between providers (dark dots) and consumers (light dots).

What we find here is somewhat unsurprising: providers have more extensive chains than consumers. Specifically, providers (on median):

- Use 2.5x more products compared with consumers
- Have 2.4x more providers compared with consumers
- Have a product category portfolio that is 26% broader than consumers
- Have 10x more internet-facing assets compared with consumers

This larger supply chain does not just mean more complexity for the business: it means an increased attack surface. Each member of an organization's supply chain is another set of products and technologies that may have their own insecurity. Attackers only have to find one of these insecurities to achieve their goals, so as the number of potential avenues for attack increases, it becomes harder to secure them all.

Key Point
Providers have a larger digital supply chain compared with consumers, presenting a much larger potential attack surface.

Providers may themselves need larger supply chains to maintain their business functions, though this also might be a reflection of the fact that discovering relationships with larger companies is easier, so our data is slightly biased in that direction. Before we move on, let's take a quick glance at the full complexity of the global supply chain via a hairball (I mean, a network) in Figure 3.

Network diagrams like this often border on useless, but it does allow us to see that the overall supply chain network relies on a tangled web of dense connections. There are further observations to be made about these last two figures. First and foremost, while a supply "chain" is a helpful metaphor, it is of course a supply network, with layers of connections and reconnections. Your organization's providers utilize each other, and their providers likewise might utilize you. Figures 2 and 3 tell us a little bit more about what this network looks like. In particular, the fact that providers have more connections and that our "hairball" in Figure 3 is so tightly woven together indicates that high importance providers are likely to be connected to one another. We won't explore this particular complexity further here, but I do want to note that while much of our thinking is about single points of failures fanning out to a single layer of organizations, the reality is that disruptions cascade and reverberate across multiple paths.

Supply chains grow with the size of an organization. It's expected that larger organizations with more diverse needs are going to utilize more providers and a wider variety of product types. But what do we mean by "larger"? Is it the number of employees? Assets? Revenue? Below we examine several measures of organizational size leveraging detailed financial data on many of the organizations in our sample.

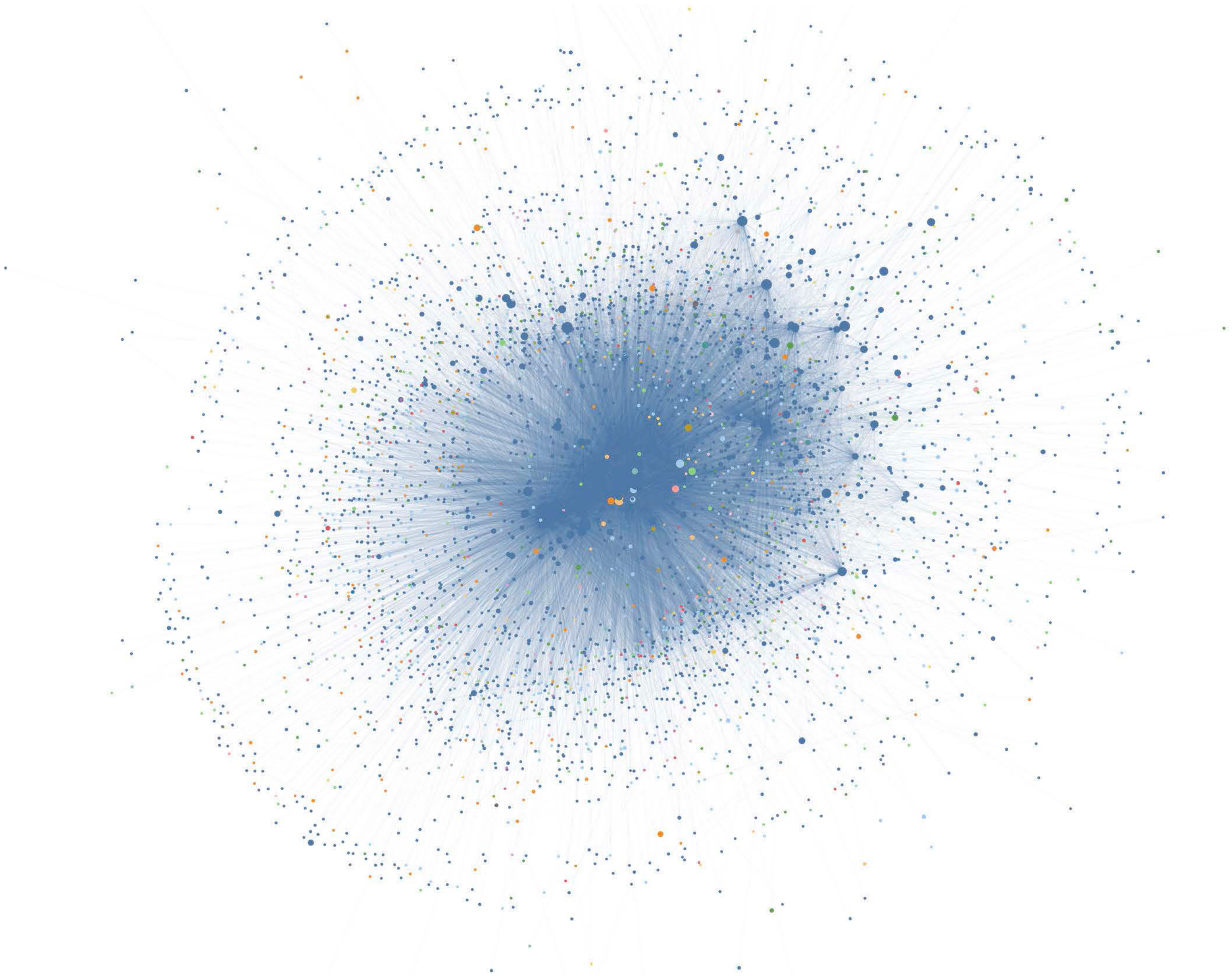


Figure 3 All of the relationships in our third-party risk management data visualized as a network.

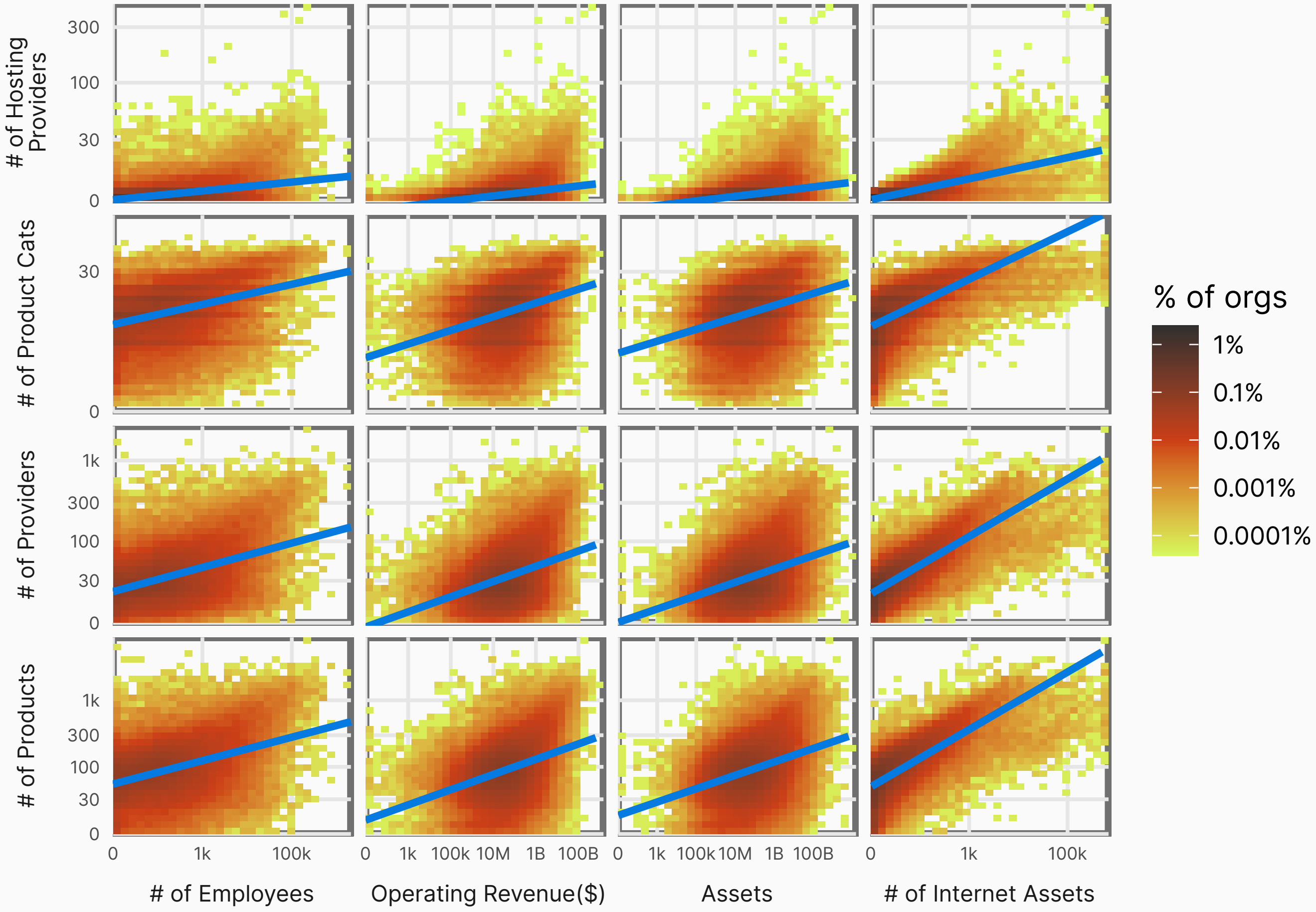


Figure 4 Correlation between organization size and various measures of supply chain size. Color here represents the density of organizations with a particular size (supply chain and otherwise). The blue lines are a linear regression indicating a positive correlation in all panels.

What sticks out in Figure 4 is that there are organizations with dozens of employees but digital footprints that can be measured in tens of thousands of active IP addresses. Similarly, we can see organizations with minimal operating revenue but thousands of products. Tech's ability to scale resources quickly means that a small organization's digital footprint can be many times the size of its workforce.

Critical Supply Chain Links

The thing that folks will most likely be chomping at the bit for is exactly which providers are most utilized across the global supply chain. However, we need to work cautiously in understanding what "most utilized" means. We start with the most basic view, specifically "what proportion of organizations we track use a particular provider" (Figure 5).

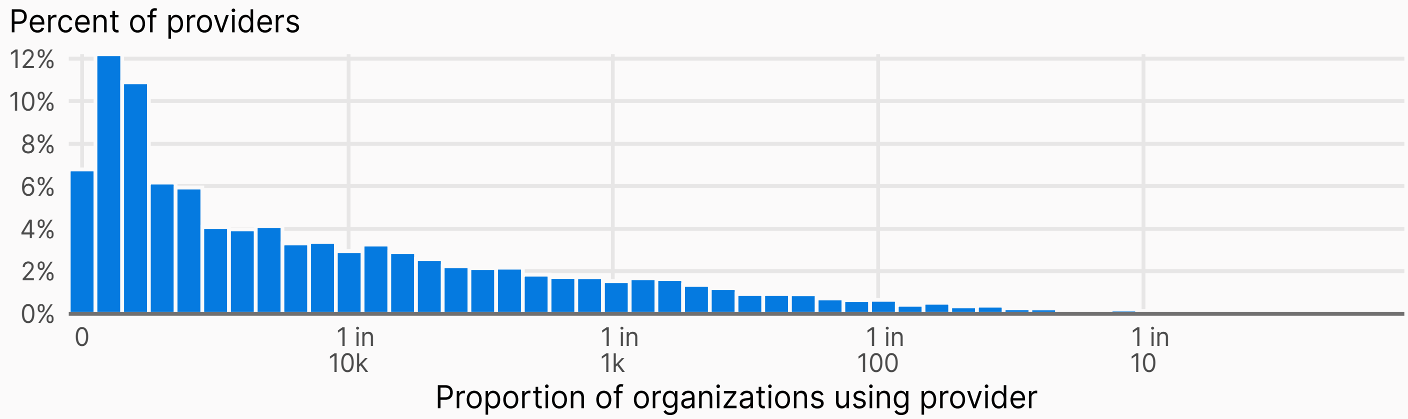


Figure 5 Distribution of proportion of organizations using a particular provider.

A large fraction of the providers in this chart are only used by a handful of organizations (less than 1 in 100,000), making them pretty sparse. Some are used by nearly everyone though, and it includes many household technology names:

- **Microsoft .** Enterprise OS and productivity software as well as cloud offerings.
- **Google.** Cloud SaaS and hosting offerings.
- **JQuery.** The ubiquitous web library that most web developers couldn't survive without.
- **Oracle.** Their database and Cloud Offerings.
- **Apache.** A wide variety of products but primarily their web hosting software.
- **F5.** Some of this is network appliances, but most is their ownership of the other large web hosting software Nginx.

But this is a simplification of the story about the supply chain. On one hand, these providers are obvious critical links, and an outage or security issue in the software they provide would be a major event. But not all consumers of these providers are the same. For example, consider the CrowdStrike outage in July 2024. One of the most impacted organizations by the incident was Delta Air Lines, the second largest airline in the US. The disruption of Delta flights had a cascading effect across a number of businesses. Meanwhile, sixth ranked (and 4x smaller) Alaska Airlines experienced no interruptions. Had the situation been reversed, the cascade effects may have been smaller.

Ultimately, what we should focus on is both the number of organizations a particular provider serves and the market share of the organizations who use that provider. For a somewhat more abstract example, consider two providers, one that serves only a few consumers, but those consumers make up 50% of a particular market, and another provider which serves the bottom 50% (by size) of all consumers. Both are likely to be critical to the global supply, but if we are simply measuring by "number of relationships," the former would not seem particularly important.

To capture this, we can calculate the market share of a provider in our supply chain data. That is, we calculate the ratio of the total revenue of consumers of that provider divided by the total revenue of all consumers in our data. If we use this number to define how "critical" a provider is, then some providers that may not have appeared to be particularly important start to emerge as critical links in the global supply chain.

[1] There is another conversation to be had not just about a consumer's size, but also their criticality. For example, a nuclear power plant might have 500-800 employees, far less than the 1,247 employed by the Manchester United Football Club, but an incident that caused a disruption for the power plant would likely be more impactful than one that cancelled a football game, though the fans might not think so.

What organizations qualify as "critical" is a policy question that is beyond the current research scope.

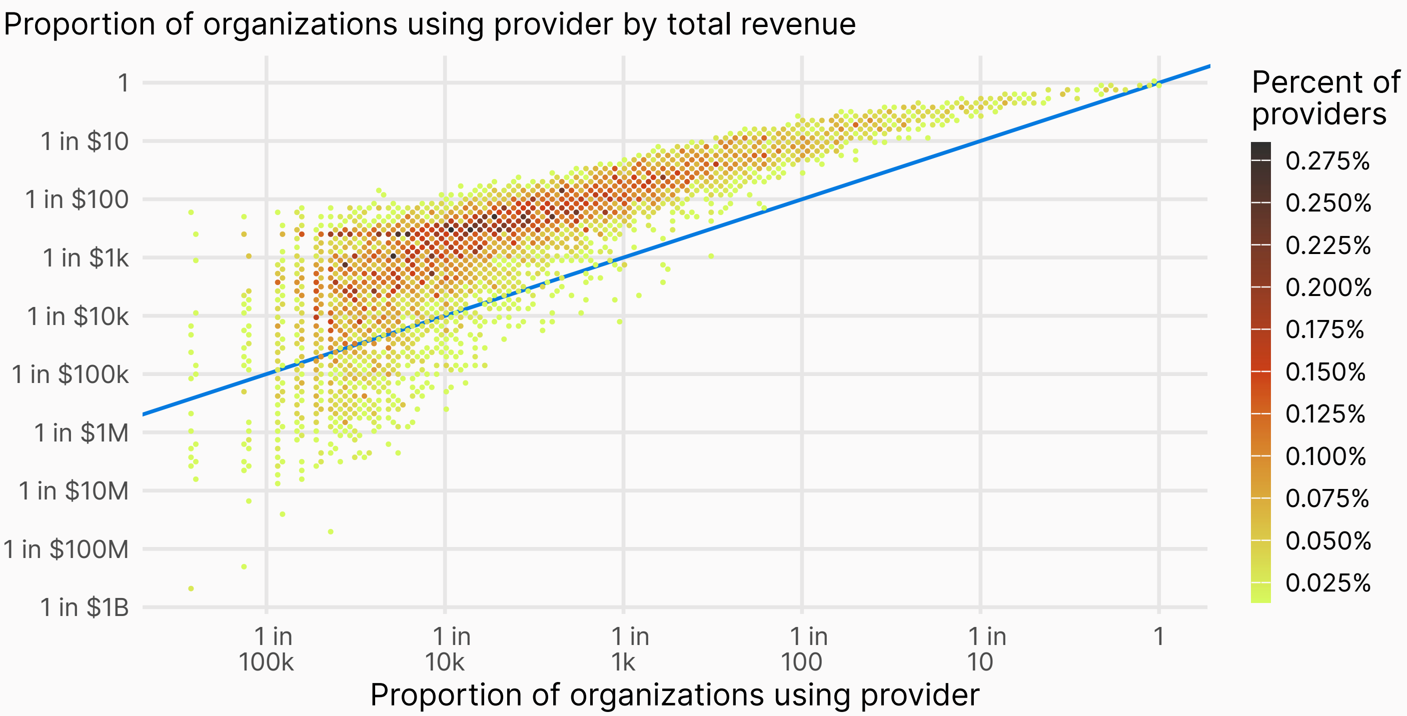


Figure 6 Comparison of proportion of organizations using a particular provider. The blue line is the "break even" line. We note that most providers, when weighted by revenue actually have a higher market share than their raw company count.

Let's take a tiny slice of that graph in a place that might be interesting. In particular, if we examine just providers who have less than a 2% market share based on total companies using that provider, but more than 20% by revenue, we get some surprising/ not surprising results in Figure 7.

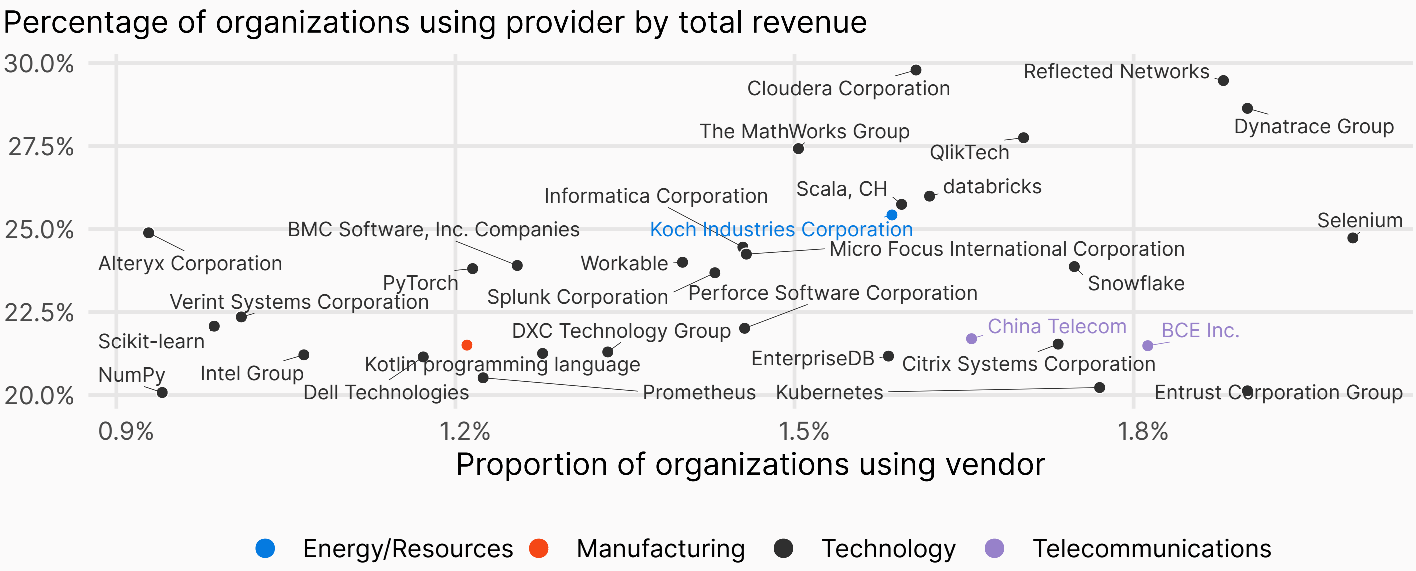


Figure 7 A sample of hidden pillars of the global supply chain, i.e. providers that are used by a small subset of very large companies.

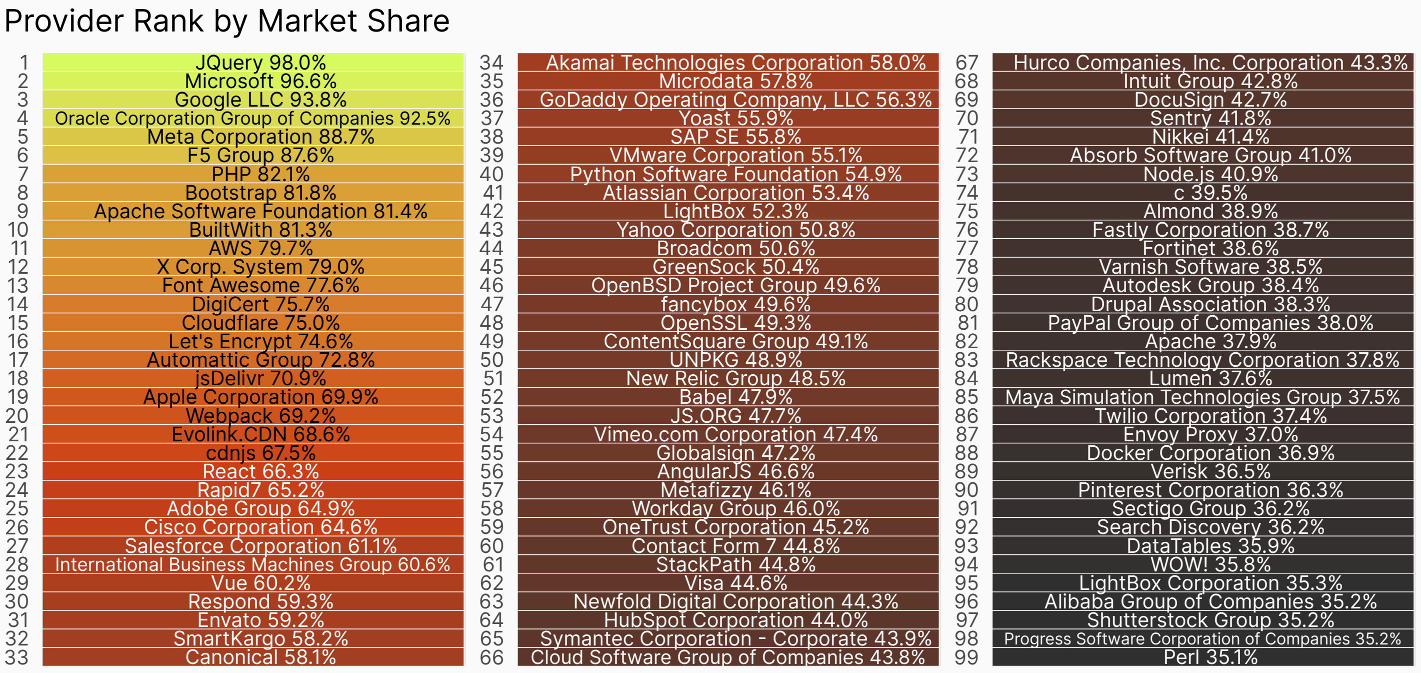
What's clear above is most of these hidden pillars of the global supply chain are in the tech sector. There are more than a few data analytics, software, and processing companies (and open source projects) included in that plot (i.e. Cloudera, Mathworks, NumPy, PyTorch). ICS technologies and energy supply are increasingly viewed as critical points in the supply chain, along with places where cybersecurity needs to be made a priority. As we move forward, we are going to use the term "Market Share" to indicate that we are examining how critical a provider is weighted by revenue.

Now that we have the appropriate measure, let's look at the top 99[2] providers in our data set[3].

We won't spend time elaborating on the particular order or location of providers in Figure 8, and instead invite the reader to find those that they might use. There are the usual players at the top (such as Javascript libraries, Microsoft, Google, Oracle). While these providers are used the most, they present very different risks in both variety and impact. Meta is included because most organizations utilize their various tracking and ad services (same with X). If these providers fail, it's probably unlikely that many organizations would be affected, other than the failure of some widgets on the webpage loading. As mentioned in footnote 1, measuring the criticality of a particular provider is difficult.

Key Point

Some providers only serve a small number of companies, but a large portion of the global supply chain when the size of the customer revenue is considered. We call these hidden pillars of the global supply chain because these hidden pillars are critical to the global supply chain but may not appear so based solely on the number of customers they serve.



Provider Rank by Market Share

1	JQuery 98.0%
2	Microsoft 96.6%
3	Google LLC 93.8%
4	Oracle Corporation Group of Companies 92.5%
5	Meta Corporation 88.7%
6	F5 Group 87.6%
7	PHP 82.1%
8	Bootstrap 81.8%
9	Apache Software Foundation 81.4%
10	BuiltWith 81.3%
11	AWS 79.7%
12	X Corp. System 79.0%
13	Font Awesome 77.6%
14	DigiCert 75.7%
15	Cloudflare 75.0%
16	Let's Encrypt 74.6%
17	Automattic Group 72.8%
18	jsDelivr 70.9%
19	Apple Corporation 69.9%
20	Webpack 69.2%
21	Evolink.CDN 68.6%
22	cdnjs 67.5%
23	React 66.3%
24	Rapid7 65.2%
25	Adobe Group 64.9%
26	Cisco Corporation 64.6%
27	Salesforce Corporation 61.1%
28	International Business Machines Group 60.6%
29	Vue 60.2%
30	Respond 59.3%
31	Envato 59.2%
32	SmartKargo 58.2%
33	Canonical 58.1%
34	Akamai Technologies Corporation 58.0%
35	Microdata 57.8%
36	GoDaddy Operating Company, LLC 56.3%
37	Yoast 55.9%
38	SAP SE 55.8%
39	VMware Corporation 55.1%
40	Python Software Foundation 54.9%
41	Atlassian Corporation 53.4%
42	LightBox 52.3%
43	Yahoo Corporation 50.8%
44	Broadcom 50.6%
45	GreenSock 50.4%
46	OpenBSD Project Group 49.6%
47	fancybox 49.6%
48	OpenSSL 49.3%
49	ContentSquare Group 49.1%
50	UNPKG 48.9%
51	New Relic Group 48.5%
52	Babel 47.9%
53	JS.ORG 47.7%
54	Vimeo.com Corporation 47.4%
55	Globalsign 47.2%
56	AngularJS 46.6%
57	Metafizzy 46.1%
58	Workday Group 46.0%
59	OneTrust Corporation 45.2%
60	Contact Form 7 44.8%
61	StackPath 44.8%
62	Visa 44.6%
63	Newfold Digital Corporation 44.3%
64	HubSpot Corporation 44.0%
65	Symantec Corporation - Corporate 43.9%
66	Cloud Software Group of Companies 43.8%
67	Hurco Companies, Inc. Corporation 43.3%
68	Intuit Group 42.8%
69	DocuSign 42.7%
70	Sentry 41.8%
71	Nikkei 41.4%
72	Absorb Software Group 41.0%
73	Node.js 40.9%
74	c 39.5%
75	Almond 38.9%
76	Fastly Corporation 38.7%
77	Fortinet 38.6%
78	Varnish Software 38.5%
79	Autodesk Group 38.4%
80	Drupal Association 38.3%
81	PayPal Group of Companies 38.0%
82	Apache 37.9%
83	Rackspace Technology Corporation 37.8%
84	Lumen 37.6%
85	Maya Simulation Technologies Group 37.5%
86	Twilio Corporation 37.4%
87	Envoy Proxy 37.0%
88	Docker Corporation 36.9%
89	Verisk 36.5%
90	Pinterest Corporation 36.3%
91	Sectigo Group 36.2%
92	Search Discovery 36.2%
93	DataTables 35.9%
94	WOW! 35.8%
95	LightBox Corporation 35.3%
96	Alibaba Group of Companies 35.2%
97	Shutterstock Group 35.2%
98	Progress Software Corporation of Companies 35.2%
99	Perl 35.1%

Figure 8 Top 99 providers weighted by revenue to determine the proportion of the market share they serve.

[2] Why 99 and not a nice round 100? Because that allows us 3 columns that look nice and are evenly divided. In other words: aesthetics.

[3] The clause "Our data set" is doing a lot of work here. You may examine Figure 8 and wonder where your favorite provider or competitor or you yourself are. Maybe some of the ordering feels wrong. These are valid questions. Any view of the global supply chain is going to be incomplete and ours is no different. It's possible the product or service that you are most interested in is not easily visible through our data gathering techniques, whereas an alternative is easier to find. Our data is going to be focused on digital products and services (though not exclusively). However, we can be perfectly candid in saying this list is not a perfect reflection of reality (no data sample is), but we are firm in our conclusion that these providers are absolutely critical to the global supply chain.

The criticality of these top companies has not escaped the notice of regulators. In the past, regulators have targeted Microsoft over the monopolization of the web browser market, and are currently trying to restore competitiveness to the online search market with actions against Alphabet Corporation. While these are generally framed as efforts to break up monopolies they may have the effect of reducing concentration risk in the global supply chain.

Of course, different organizations have different needs, and so the popularity of products is unlikely to be the same for Aerospace/Defense contractors as it is for Retail organizations. Figure 9 examines providers that "punch above their weight"[4] with respect in a particular industry.

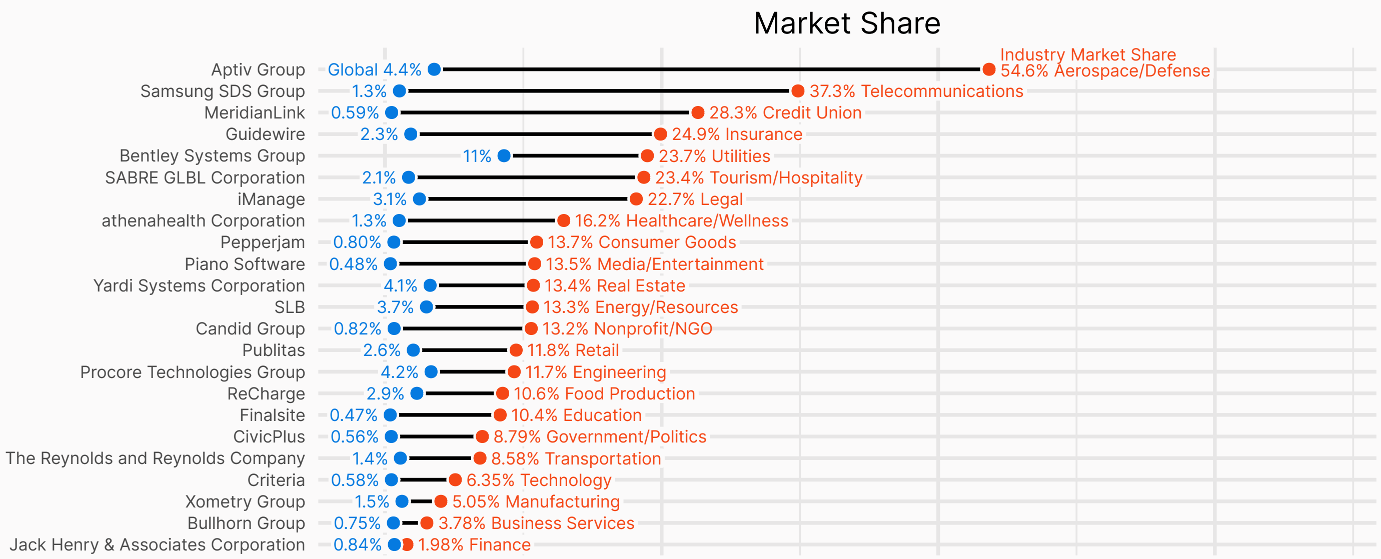


Figure 9 Industry market share comparisons.

What's striking in Figure 9 is that some of these companies make up a small percentage of the global market share but a large fraction (in the case of Aptiv Group and Aerospace a majority!) of the market share in a particular sector. Many of these providers make niche products that dominate a particular market segment, making them critical to that segment. For example:

- **Digital Lending Platforms.** A platform supporting one-third of global financial institutions, including credit unions, could experience an incident, disrupting financial operations, delaying loan approvals, and exposing sensitive customer data.
- **Infrastructure Software for Utilities.** A software solution managing 25% of global utility infrastructure could experience an incident, leading to cascading effects such as service disruptions and safety risks.
- **Real Estate Management Platforms.** A property management and rental payment platform is essential for tenants and landlords, where an incident could prevent rent payments, disrupt cash flows, and create financial uncertainty.

[4] In particular, for each sector we looked at the ratio of the percentage of companies within a particular sector a provider serves vs the percentage of the global companies. For each consumer sector we then take the top company.

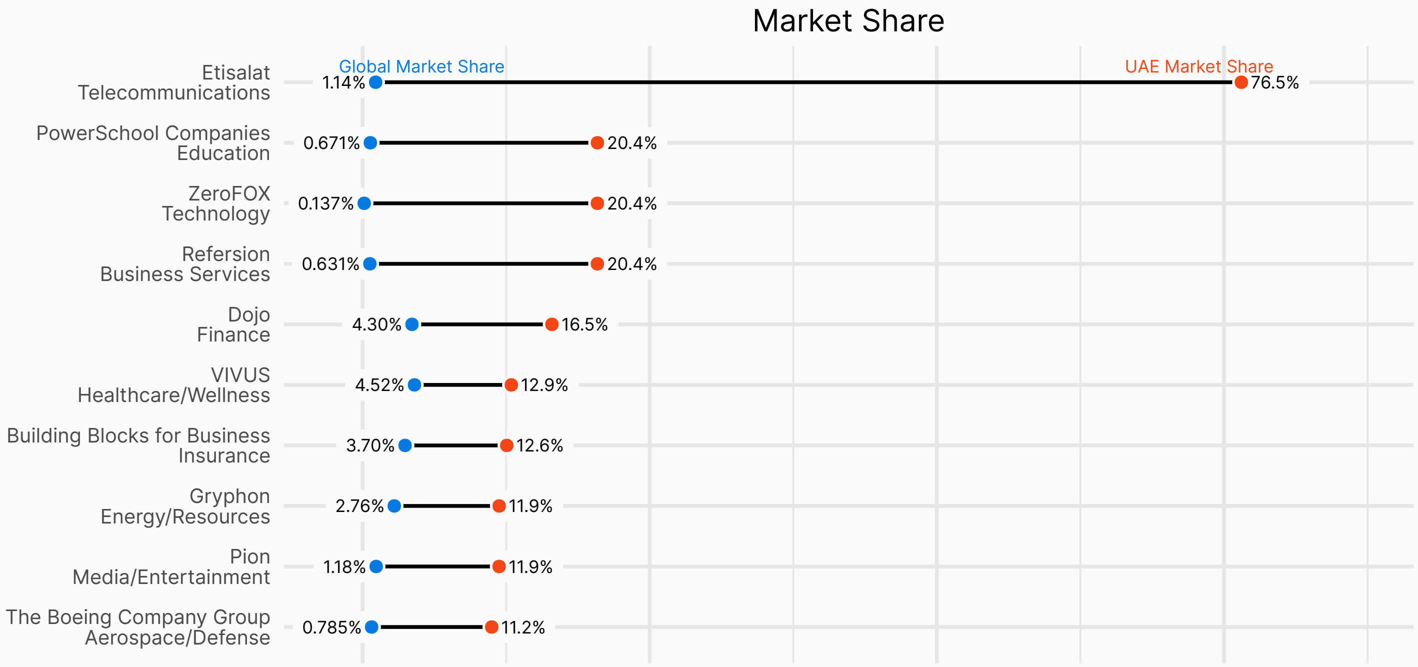


Figure 10 UAE market share compared to global market share.

There is nothing special about sectors and we can do the same for any particular country. For example, if a country is particularly dependent on a single provider, incidents may lead to a major national, but not a global disruption. One particular example is a recent data breach exposed PowerSchool students' sensitive information. In our data, Powerschool does not have particularly high global market share, less than 1% of the global education market. However, in the United Arab Emirates (UAE), they are highly represented, serving ~20% of the UAE education market. Figure 10 outlines other providers across various industries that are critical to the UAE.

Some of the providers are unsurprising. Etisalat is the local telecom and mobile provider; it follows that the global market share would be low while the in-country market share would be nearly universal. But just as niche providers in particular industries can have an outsized presence, the same can be said for providers within a particular geography. This is something Bitsight has visibility into.

A related query might be what providers in a specific country serve a large proportion of the global supply chain. Recently, US policy has considered banning products from Russia and China, or requiring the sale of foreign-owned assets as was the case with TikTok (parent company ByteDance). Many Chinese companies have significant global market share, obviously complicating the various political choices (Figure 11).

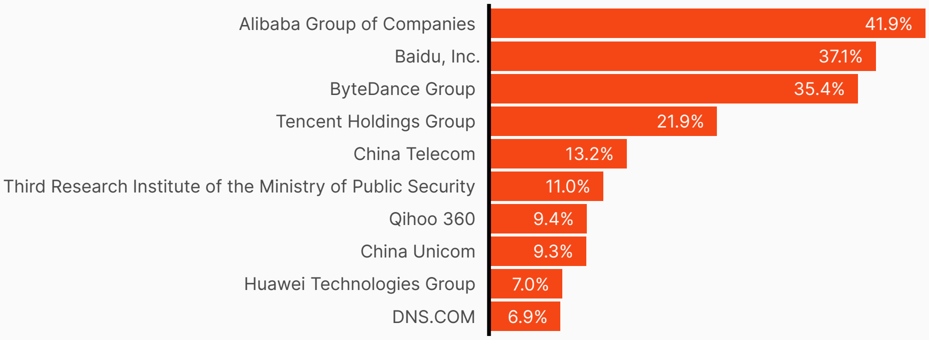


Figure 11 Top Chinese providers to the US supply chain.

Key Point
Providers may have a small global market share, but an outsized presence in a particular sector or geography.

Indeed, five of the above companies (Tencent, China Telecom, Qihoo, China Unicom, and Huawei) are designated by the US Department of Defense as "Chinese Military Companies operating in the United States". The "Third Research Institute of the Ministry of Public Security" is explicitly a branch of the Chinese domestic government. Nearly every other organization on the above list has had some links to the Chinese Military and has been considered for some form of regulation by the US government, with a potential ban on TikTok (ByteDance's main product in the US) working its way through the US court system.

Key Point
33% of the US supply chain relies on companies listed by the US Dept of Defense as a "Chinese Military Company." Two-thirds of the US supply chain relies on the companies in Figure 11.

Whether providers are serving a particular niche or not, knowing more about how these providers operate is critical. One obvious hypothesis is that larger companies will have more market share, but we are also curious about whether more technologically inclined companies might have higher market share. Organizations who have explored further down the "digitization" path are likely to have a larger attack surface and may be more prone to cyber incidents. As a rough measure of digitization, we look at the number of internet-facing assets per employee. We examine both these hypotheses in Figure 12.

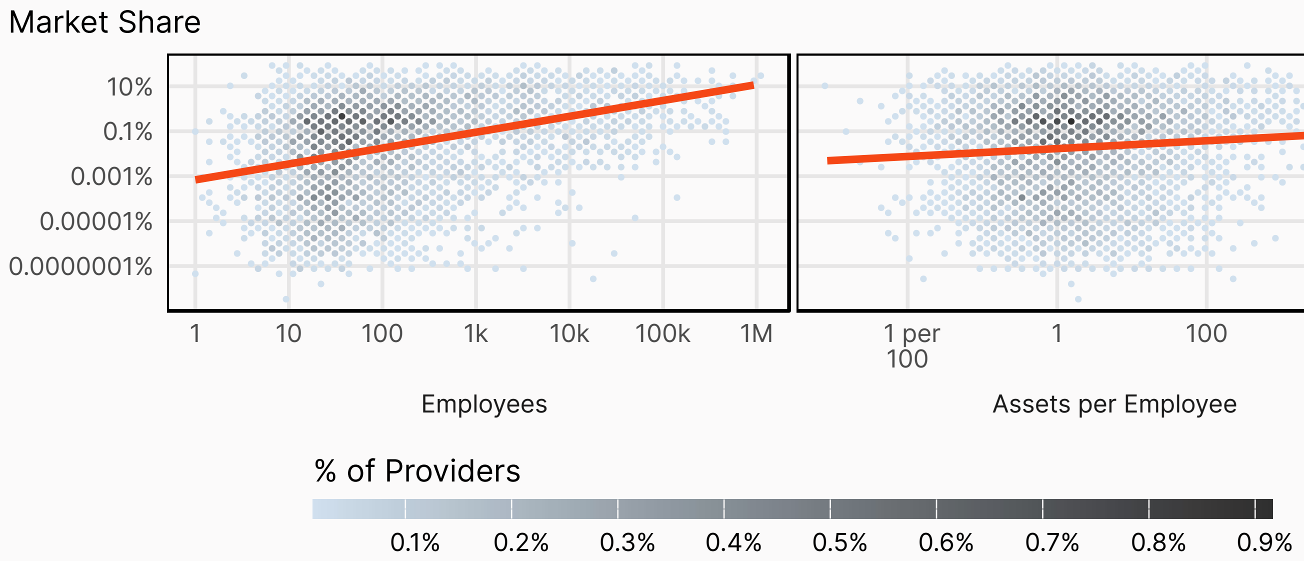


Figure 12 Digitization and organizations and market share.

Figure 12 indicates that provider size and level of digitization do correlate with the market share, though weakly with assets per employee. In particular, larger organizations tend to have larger market share, an unsurprising result given we expect as companies grow that their relationships will grow both in the number of customers and the size of those customers. There are exceptions though, that is, organizations that have only a handful of employees, but have a very high market share. Perhaps unsurprisingly, among them are popular web frameworks Angular and React, open source, widely used with large company backing (Google and Meta respectively), but with a small team of custodians.

[5] Forthcoming research will examine this in far more depth.
[6] This does significantly correlate based on spearman's rho correlation coefficient.

On the right-hand side there is a weaker positive correlation. Organizations that are more digitized tend to have larger market share. Because we are examining "assets per employee" this is at least somewhat orthogonal to the total number of employees. This certainly seems to make sense given how revolutionary computing has been in the last century and our data focus on technology. Again, the correlation is not strong and there are examples of sparsely digitized organizations serving a large segment of the market. Some examples serving more than 10% of the global market with high levels of digitization are analytics companies monitoring cloud (Zabbix, Hashicorp), customer data (Amplitude, SnowPlow, Tradedesk, DoveCot), AI (Amplience), and Blockchain (Elliptic).

Key Point
In the global supply chain, critical organizations with large market share may have just a few dozen employees.

Security Performance in Critical Supply Chain Links

The next pressing question is to examine how well companies fare in their cybersecurity posture. A critical company with a large digital footprint and a high number of security issues could prove a blinking red light for our digital supply chain.

It's worth it to take a second to point out that larger, more digitally forward providers are going to have more systems and therefore, more exposures. These organizations are often required to have best in class compensating controls and security processes that prevent major incidents.

This is still an area in which we at Bitsight tread carefully, as we don't want to guide attackers to critical infrastructure, so we'll stop short of indicating who is both a critical supply chain player and less than perfect at security. The first step in our analysis is to ask if providers are better or worse at security compared to consumers.

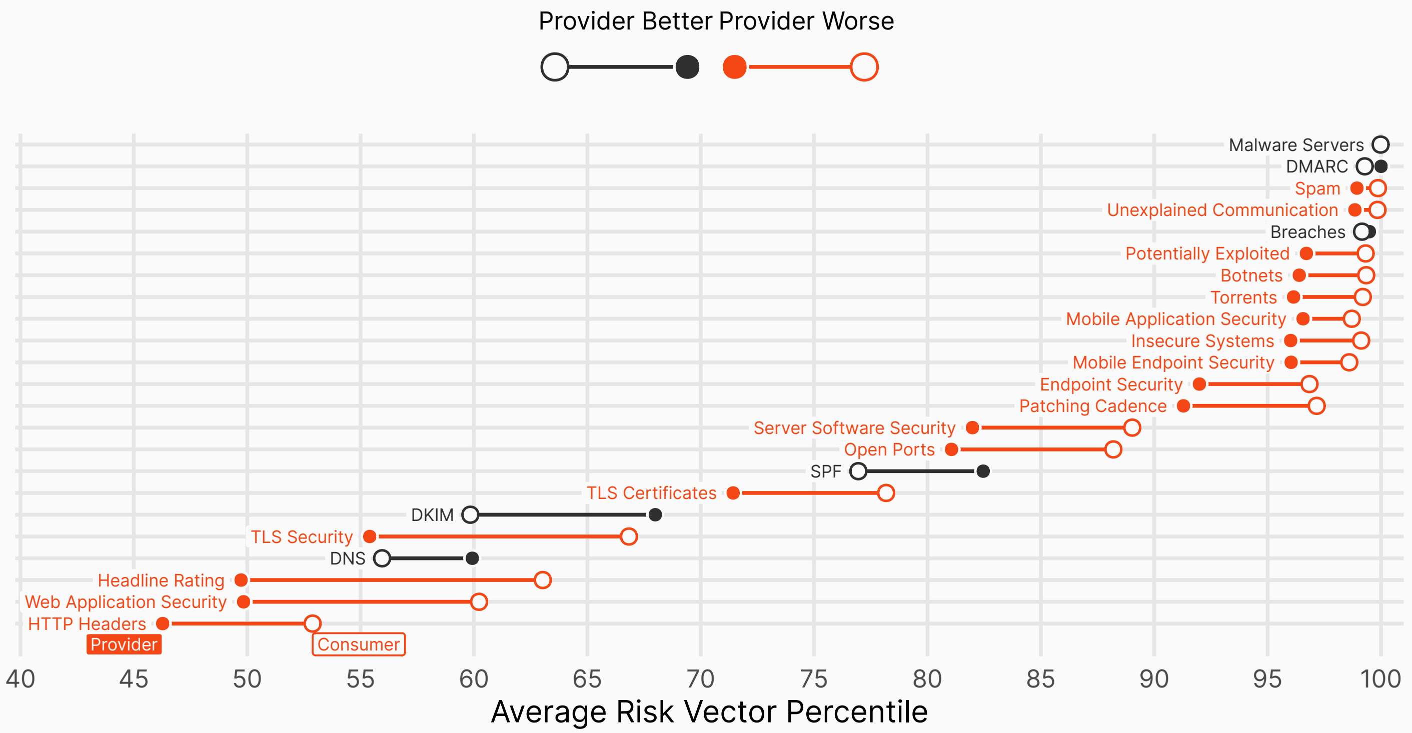


Figure 13 Average risk vector scores for providers and non-providers in our data set. (A note about the term "non-provider:" recall from the introduction that every organization is a "provider" in the sense that they provide products and/or services within an economy, but we have already made the distinction here between those we classify as providers and have links to in our data, and those that we don't.)

On average, providers tend to have slightly lower security ratings than consumers, with differences of up to 20% in 16 of the 22 Bitsight risk vectors analyzed. Notably, providers perform better in four of the six vectors related to security standards (DMARC, SPF, DKIM, and DNSSEC), which aligns with expectations for larger, more tech-focused organizations. Considering these observations, we can consider a few root causes for the consistent difference in performance by providers and consumers:

1. Providers leverage digital infrastructure as a means of business, as such they will have a greater digital footprint and therefore more digital risk [Gallagher Re's Scanning the Horizon | Bitsight].

2. There is a potential risk transfer occurring, where, when providers are solving specific business problems for consumers, they are also absorbing the cyber risks associated with the problems.

3. Providers tend to have a higher volume of exposures, and better compensating and reactive controls.

The next hypothesis to test is exactly which providers have lower scores. The hope would be that its providers with a small market share, only serving a handful of customers who are the ones in the bottom. However, the answer seems to be no. In the interest of simplifying things a little bit, we'll divide the Bitsight Headline rating into the top and bottom percentiles in Figure 14.

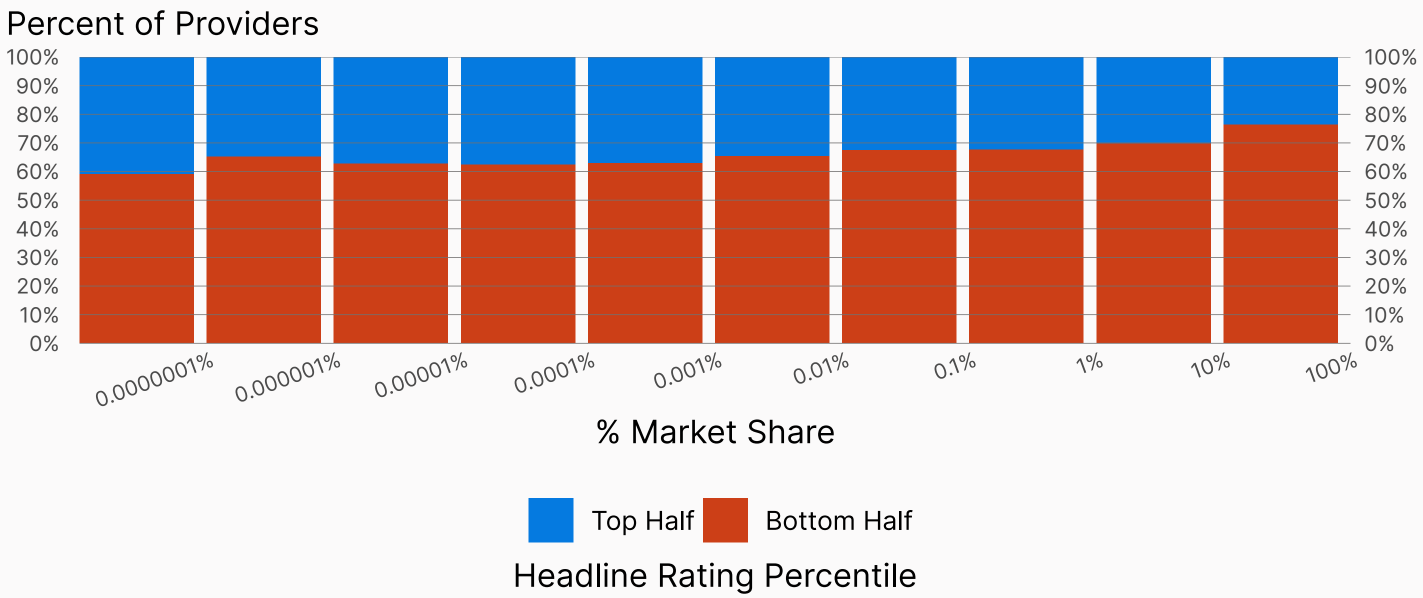


Figure 14 Letter grades of providers across various levels of market penetration. Dashed lines through the bar represent the overall distribution of letter grades for all organizations.

What Figure 14 makes clear is that, regardless of how prominent a particular provider is within the supply chain, some are in the bottom half of the field (and the top!) when it comes to security posture. Typically, as market share increases there is also an increase in digital infrastructure, risk transfer, and security findings, but this comes with more funding, better talent, more mature reactive processes, and more sophisticated compensating controls.

Key Point

Large providers (and providers in general) tend to have worse security posture than the overall population of organizations that Bitsight monitors.

So, based on Bitsight's risk vectors, who are those critical global supply providers that don't have the best security posture? We aren't going to name names here for fear the bad guys will focus on them for maximum disruptive value, but we'll refer to them in generic terms:

1. Two SaaS and enterprise modeling software providers
2. A European Manufacturing corporation
3. Several network device suppliers
4. A shipping a logistics company
5. A large Payment Processor

Let's move beyond the headline rating and toward some details into the actual ratings. One measure of security posture is the rate at which new findings develop for various providers. Each finding could be the entry point for an attacker, so the more findings an organization has, the more worried we might be. However, we also acknowledge that organizations with a larger attack surface (i.e. more internet-facing assets) are more prone to having findings. To pull these ideas together into one measure, we examine the number of new findings per provider, per publicly facing asset for a few of the mentioned risk vectors in Figure 15.

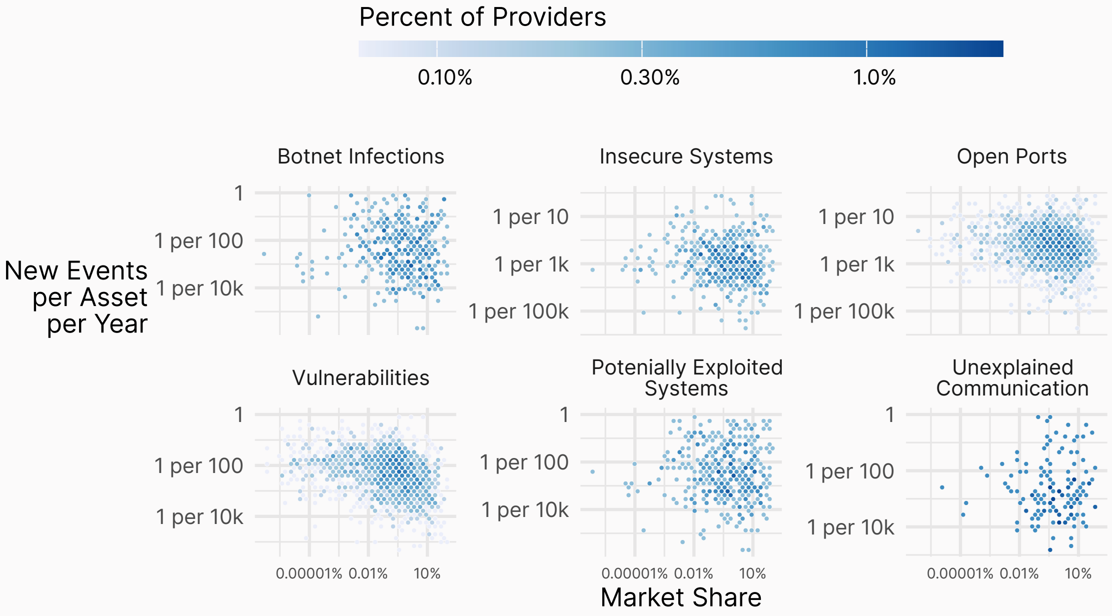


Figure 15 New Event rates for providers vs market share.

The lack of correlation here is the story. Regardless of market share there are providers who have extremely high and low event rates. We note that the selected risk vectors here present real, immediate risk to organizations that are either current infections (Potentially Exploited, Botnet Infections, unexplained communication) or exposed security risks (Open Ports, Vulnerabilities, Insecure Systems):

- An EMEA transportation company with 20% global market share has an insecure system rate in the worst 25% (in a year, 1 in 3400 systems has an insecure system finding).
- A US based marketing corporation has 14% global market share in the worst 25% botnet infection rate (in a year, 1 in 3,000 systems would have a botnet infection).
- An APAC manufacturing company has ~10% global market share and is in the worst quartile for open ports (1 in 6500 assets has a negative open port finding).
- A Fortune 500 energy company with 34% global market share in the worst quartile of insecure systems.

For one of these risk vectors, patching cadence, the event rate is only part of the signal. The other major signal is the time it takes to remediate the vulnerabilities. So let's try to focus our attention and examine all of these things at once.

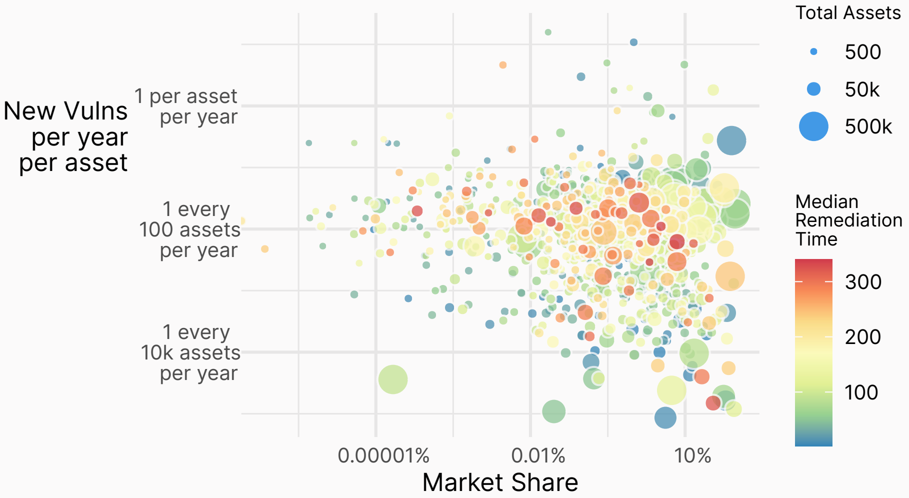


Figure 16 New Event rates for providers vs market share.

Key Point

There are providers with large market share that are among some of the worst performing security organizations.

There is a correlation here between very large organizations (measured by number of assets) and the number of events per day (larger bubbles tend to be located higher vertically). The critical bit is that there are providers with a large number of assets that have open vulnerabilities for a relatively long period, a large attack surface with respect to the number of assets, and serve a large portion of the global supply chain. Truly a recipe for supply chain risk.

One question to answer from that chart is "are there companies with particularly high risk profiles?" And the answer is unfortunately, yes. A couple of examples:

- An EMEA manufacturing company with long-standing open vulnerabilities (many over three years old), with five new vulnerabilities added per day, more than 181k assets on the open internet, and is involved in 26.5% of the global supply chain.
- A US data center company that takes longer than a year to fix the typical vulnerability, with four new vulnerabilities per day, serves more than 10% of the global supply chain, and has more than 47k publicly facing assets.

These companies may present a real threat to the global supply chain and could very well be the nexus of the next major supply chain incident.

Key Point

There are major supply chain players (>25% market share) that have a large market share, a large attack surface with many vulnerabilities, and exceptionally long remediation times for those vulnerabilities.

Conclusions and Recommendations

We've traversed many supply chain links in the preceding pages. What we hope to convey the most here is that the "supply chain" is not really a chain at all. A chain implies a series of linear, uniform, interconnected links, each as prone to failure as the next (if the chain is any good, that is). But what the global supply chain really resembles is a complex web of connections, with unexpected nexuses that have high variability with respect to their security posture.

We must note that any sort of scientific investigation like this requires us to take a step back and understand how we might be missing the complete picture. As we noted in the text, it is nigh impossible to see the totality of the global supply chain, and the providers we examine here are more likely to be larger and more tech focused in their offerings. While incomplete, it does mean we are more likely to capture and evaluate critical providers in the cyber portion of the supply chain, which was the ultimate goal of this study.

Additionally, while we have identified critical providers in the sense that they serve a large portion of the global supply chain (or a particular industry), their services might not be critical in the day-to-day running of an organization. The economic impact of being unable to track web advertisements would likely break a few things, but it would be unlikely to grind any particular portion of the economy to a halt. But assessing the criticality of providers at scale remains a challenge for future work.

Finally, one portion of the supply chain that we've skirted is the notion of how risk might be concentrated in various cloud providers. Unlike the above, we do have visibility into cloud usage, including among providers, what cloud regions they operate in, and even the services they offer. There is much more to come on this, but it is another layer of complexity that wouldn't quite fit in this already substantial report.

If the global supply chain is a tangled web of providers of physical goods, software, services, and hosting, then this is also true of any particular organization's supply chain. It's likely smaller, but still likely dauntingly large. So what is a CISO or risk manager to do in the face of this complexity?

- **Enumerate your supply chain**. Knowing is half the battle, and the first step here is understanding who is enabling your organization's mission.
- **Evaluate criticality.** Every piece of equipment, software, and data your company utilizes was selected after due consideration. But some are more critical than others. A gap in marketing analytics will not be quite as devastating as a major cloud provider shutdown.
- **Assess your providers' security.** The first step to knowing who your critical providers are is to understand their security posture. Bitsight can of course help to identify how these organizations are doing with outside assessments.
- **Reach out.** These providers may not have a clear view of their own security issues. Bitsight includes the ability to Enable Vendor Access, a process in which you can share findings about one of your providers with that provider so they can in turn improve their security posture (and the continued operation of your business).
- **Look deeper.** With your third-party network on its way to better security, it's time to examine how your extended supply chain is fairing. Are your most critical providers themselves dependent on a less-than-secure third party (fourth party to you) provider? In this case, it may be time to evaluate what you can do for the fourth party, or maybe shore up your own resources with redundancy.
- **Evaluate your own criticality.** If your own organization is a critical player in the global supply chain, then it's possible that an incident could not just affect you, but also disrupt the supply chain in a way that could be orders of magnitude more costly than the incident itself.

If you're looking to better understand and manage cybersecurity risks, reach out to Bitsight. Our cyber risk intelligence solutions empower you to rapidly identify exposure, detect threats, and communicate and mitigate cyber risk. Bitsight insights fuel better decision-making and risk mitigation across your extended attack surface. In addition, Bitsight has industry-leading insights on countries, locales, and critical national infrastructure.

Get started with a free vendor risk assessment for up to 20 vendors, giving you visibility into the security posture of your supply chain.

Methodology

This analysis relies on data from three different data sources collected by Bitsight.

1. **Fourth party relationship data.** This consists of known relationships between entities and the products/services they leverage. This data is both derived from first-party data collected by Bitsight, as well as other services. We err on the side of "this relationship exists" when there is possible noise, as we think organizations would want the most expansive view of their potential supply chain.
2. **Organization data.** One of Bitsight's strengths comes from its ability to not only identify internet assets, but who ultimately owns and controls them. This "entity" data is further enriched with firmographic data allowing Bitsight to know not just the technologies and potential security issues with an asset, but who is responsible for them. We combine this with external firmographic data from other sources to derive a more complete picture of an organization's features.
3. **Events data.** Security data is derived from the wide variety of Bitsight's security assessment technologies, which examine an organization's diligence in maintaining good security hygiene, evidence of current compromise, and history of past incidents.

The results in this research are derived from a snapshot of data collected at the end of October of 2024.

Bitsight TRACE is Bitsight's security research and intelligence team. Composed of researchers and threat analysts with deep cybersecurity experience, the team investigates and publishes information on emerging malware, vulnerabilities, and threats. Our researchers leverage Bitsight's extensive cyber data collection, mapping, and attribution technology to not only investigate security incidents, but oftentimes identify a range of vulnerabilities and threats. The research is used throughout the security community to improve cyber readiness.

sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BITSIGHT