Industry Titans Battle the Beast of Supply Chain Cyber Risk

A COLLABORATIVE REPORT BETWEEN SecurityScorecard & Cyentia

Introduction

Companies among the Forbes Global 2000 stand at the forefront of economic output and influence. These corporate giants collectively account for $51.7 trillion in revenue, $4.5 trillion in profits, $238 trillion in assets, and $88 trillion in market value, underscoring their critical role in the global economy. However, with great economic power comes great vulnerability, particularly in the realm of third-party risk.

The reliance of these megacorporations on extensive supply chains opens them to significant cybersecurity challenges. Our records show that many Global 2000 organizations have directly suffered a recent breach, and nearly all of them are regularly exposed to breaches via their closest third parties. What's more, the total impact of these events is staggering.

As we explore the complex landscape of third-party cyber risk in this report, it becomes clear that no organization is too big to fail. The interconnected nature of modern business means that a vulnerability in one part of the supply chain can reverberate throughout the entire ecosystem. We aim to provide in-depth analysis of these risks, offering insights to help Global 2000 companies and their suppliers bolster defenses and mitigate the impacts of third-party cyber threats.

In the digital age, no entity is an island. The cyber resilience of these Global 2000 companies is inextricably linked to the security practices of their third–party partners. Understanding and mitigating these risks is more than just a corporate responsibility, but also an imperative for maintaining global economic stability.

CONTENTS

About the Cover

The cover design is a ode to the 1999 Japanese film, Godzilla 2000. The original release carried the tagline "Earth's most powerful monster fights a beast from outer space," and we adapted the subtitle from this. Supply chain cyber risk isn't exactly alien, but it does originate outside of organizational boundaries and has an uncanny ability to penetrate even the best defenses.

Key Findings

70% of Global 2000 companies earn solid SecurityScorecard ratings, but that leaves 30% of them struggling to maintain a strong security posture.

12% of these companies had at least one security breach during the 15-month period of our analysis.

Losses from a typical breach is tenfold higher for the Global 2000 than small businesses. Extreme events cost them 77 times more.

We estimate total losses across reported events to be between $20 and $80 billion—that's equivalent to a top 10 ranking among the Global 2000.

We identified nearly 18,000 IT products/services from 8,000 vendors that are directly used by the Global 2000.

In 69% of those third-party relationships, vendors have a weaker security posture that their Global 2000 partner.

99% of Global 2000 companies are directly connected to vendors that have had recent breaches.

On average, 20% of the third parties used by a Global 2000 firm have been breached in the last 15 months.

Each of the eight most widely deployed vendors are used by at least 80% of Global 2000 companies. 4 of the top 5 have had a recent breach.

Concentration risk is a big concern for the Global 2000. Incidents affecting multiple parties cost 17 times more than traditional single-party events.

Methodology

The Global 2000

The Forbes Global 2000 ranks the largest companies in the world using four metrics: sales, profits, assets, and market value. The 2024 list accounts for $51.7 trillion in revenue, $4.5 trillion in profits, $238 trillion in assets, and $88 trillion in market value. There's a tendency to view all the companies in the Global 2000 as equally gargantuan, but there's actually quite a bit of variation among them. This can be seen in the left chart, which plots the revenue and market value of each company on the list.

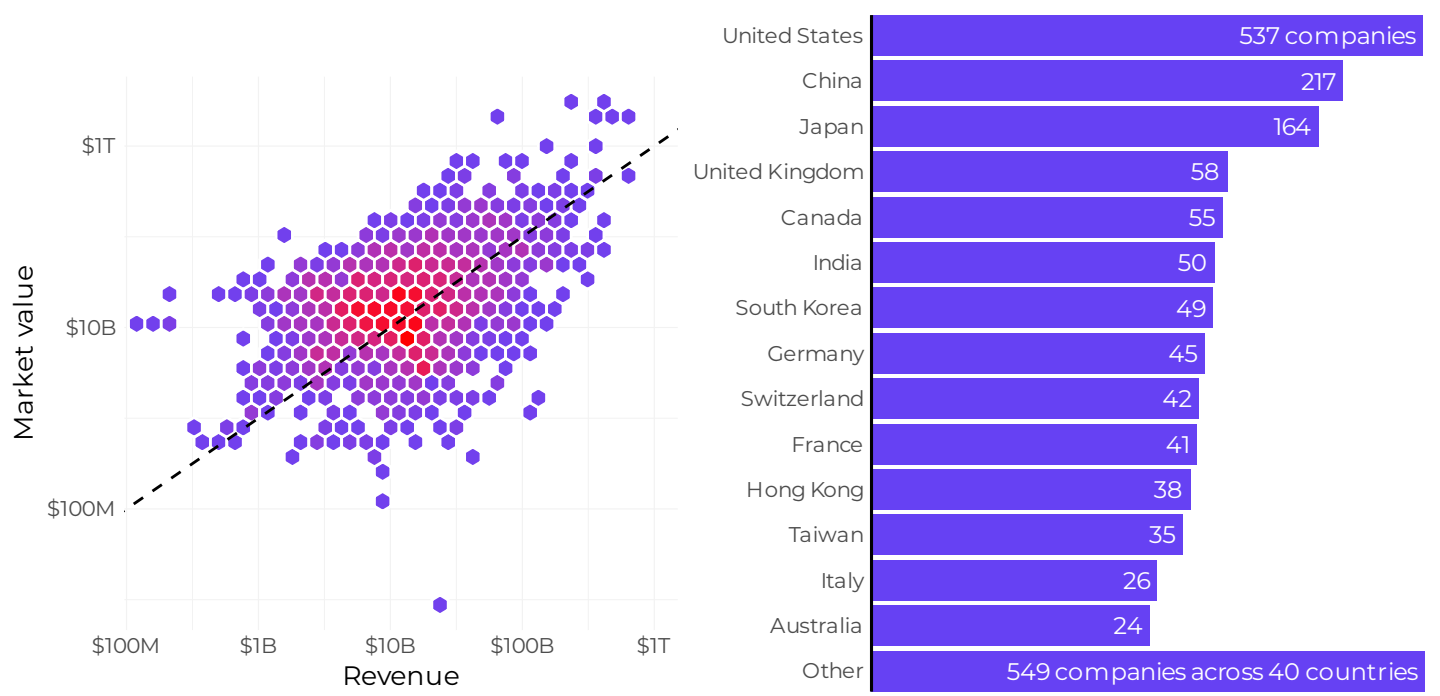


Figure I: Revenue vs. market value and country of origin

The Global 2000 also has a wide geographic distribution. In terms of company headquarters, the United States is the most represented country. China and Japan claim broad coverage as well. All told, the Global 2000 includes companies from 55 countries.

Part of our analysis will focus directly on the security posture and breach history of the Global 2000. We'll also analyze the ecosystem of third-party vendors surrounding each Global 2000 company to understand the nature of cyber risk across their supply chains.

About the Data

SecurityScorecard continuously scans the internet to identify vulnerable and misconfigured digital assets. Additionally, SecurityScorecard monitors signals across the Internet, relying on a global network of sensors that spans the Americas, Asia, and Europe. The company operates one of the world's largest networks of sinkholes and honeypots to capture malicious signals and further enrich its data set by leveraging commercial and open-source intelligence sources. In total, SecurityScorecard continuously monitors the security posture of over 12 million organizations globally.

The data on third-party relationships comes from SecurityScorecard's Automatic Vendor Detection capability. Automatic Vendor Detection identifies vendors and products that make up the digital supply chain of modern organizations. Specific to this report, we're focusing primarily on the myriad IT products and services used by the Global 2000.

> *The 2024 list accounts for $51.7 trillion in revenue, $4.5 trillion in profits, $238 trillion in assets, and $88 trillion in market value.*

331
BREACHES
FROM JANUARY 10TH 2023 TO MARCH 30TH 2024

The breach data referenced in this report also comes from SecurityScorecard's intelligence operations and covers a period starting from Q4 of 2022 through Q1 of 2024. A total of 331 confirmed security breaches were detected across the Global 2000 during this timeframe. Breaches suffered by third-party vendors of the Global 2000 are also tracked by SecurityScorecard and we'll tap into this data as we explore third-party and concentration risk.

Looking for a deeper dive on signals collected by SecurityScorecard, analysis of that data, and how we product security ratings?
You're in luck! We recently updated our scoring methodology, and it's detailed in this ebook.

Snapshot of the Global 2000 Cyber Risk Landscape

Before delving into the contours of the cyber risk landscape of the Global 2000, we'll establish a high-level view of how things look. Let's first dispel the notion that these mega corporations are immune to the cybersecurity challenges experienced by the rest of the economy. Over 70% of Global 2000 firms earn solid SecurityScorecard ratings of As and Bs, but that means there's still a substantial number of them struggling with subpar security postures.

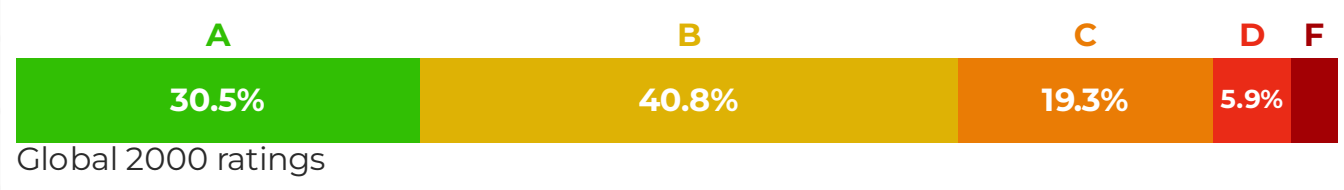


Figure 2: Distribution of SecurityScorecard ratings for the Global 2000

They're also not "too big to fail." About 12% of the Global 2000 firms suffered a known breach during the 15-month period of our analysis. But the risk landscape for organizations of this size extends far beyond their boundaries. Many of them manage huge networks of third-party vendors that have their own security struggles. As a testament to this fact, 99% of the Global 2000 are directly connected to vendors that have had breaches during this timeframe.

Figure 3: Percentage of Global 2000 and their vendors with known breaches

Do all those third-party breaches result in first-party impacts? No—but there's definitely ample evidence of incidents that impact multiple supply chain partners. Our analysis shows that these multi-party events typically have a total cost that's 17X higher than single-party breaches. That's a particularly relevant statistic with supply chains as large as those encircling the Global 2000. We'll unpack all this and more in the pages that follow.

Breaches of the Global 2000

ABOUT 12% OF THE GLOBAL 2000 FIRMS SUFFERED A KNOWN BREACH DURING THE 15-MONTH PERIOD OF OUR ANALYSIS

Let's surface some more details around the 12% of the Global 2000 that had a recent breach in this section.

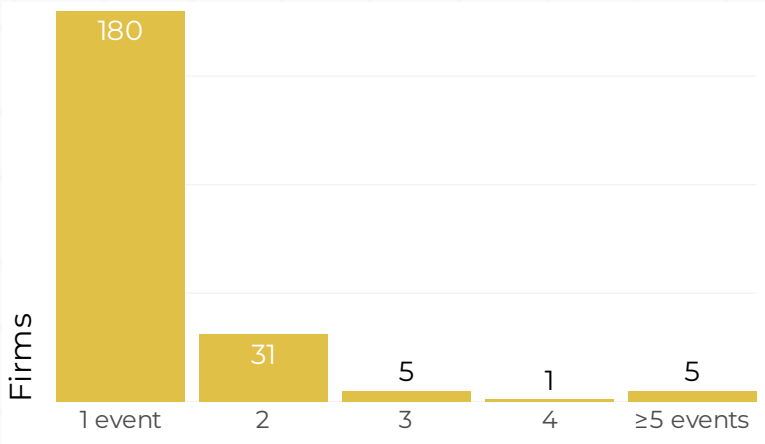


Figure 4: Number of known breaches per firm among the Global 2000

We'll start by clarifying that some (a bit under 2%) of these companies experienced more than one incident. The rate of recidivism for a handful of them was particularly high, with 5 or more confirmed breaches on the public record during the 15 month period of study. Our goal isn't to name and shame, but you likely have good guesses as to the identity of some of them if you've been keeping up with recent headlines. Among them, you'll find major software companies, large manufacturers and energy providers, giant consulting firms, national banks, and global hospitality companies.

> *Less than 2% of these firms had multiple incidents, and some had 5 or more breaches within 15 months. Major software companies, manufacturers, and national banks are on this list.*

ARE THE GLOBAL 2000 MORE OR LESS LIKELY TO SUFFER BREACHES THAN SMBS?

To answer this question, we'll leverage research conducted by the Cyentia Institute in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA). They used 10 years of historical data to estimate the annualized frequency of cyber events for firms in different revenue tiers. The results are captured in the table below.

Probability of a firm experiencing a given number of events			
Revenue category	One or more	Two or more	Three or more
Upper Bound			
More than $100B	29.33%	9.32%	3.56%
$10B to $100B	21.93%	4.91%	1.28%
$1B to $10B	17.04%	3.09%	0.71%
$100M to $1B	12.95%	1.56%	0.23%
$10M to $100M	11.53%	1.12%	0.11%

Megacorporations are 9 times more likely to encounter 2 incidents.

They're 32 times more likely to face 3 or more breaches!

The probability of at least one cyber event impacting the likes of the Global 2000 is more than double that of small to midsize firms. That may not seem like a huge difference, but notice the growing disparity for multiple breaches. Megacorporations are 9 times as likely to have 2 incidents and 32 times more likely to experience 3 or more!

The geographic distribution of breached organizations in Figure 5 is quite interesting. Numerically, the United States dominates the field. But that's not terribly surprising given that the U.S. has the largest share of organizations in the Global 2000 and expansive breach reporting regulations.

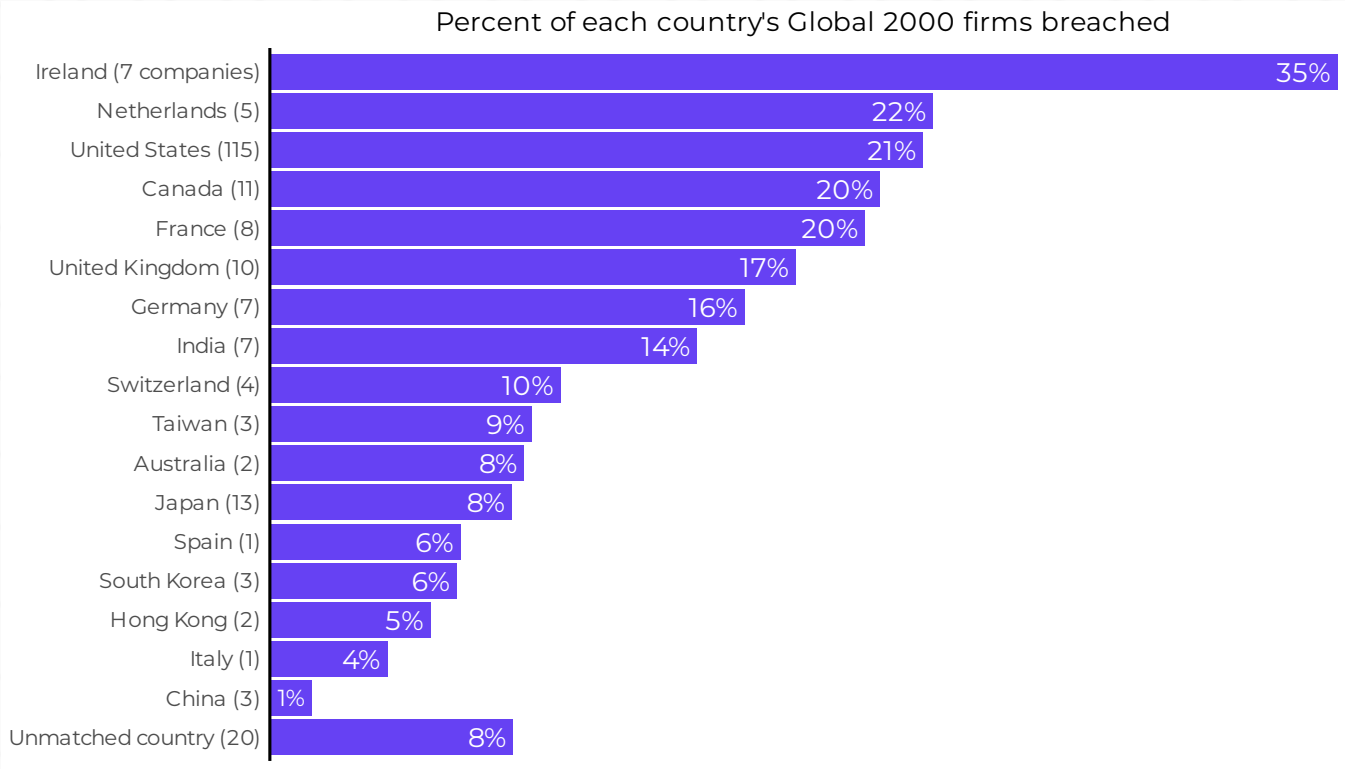


Figure 5: Countries with the highest breach rates among Global 2000 firms

Relatively speaking, however, Ireland has the highest breach rate. Over a third of the 20 Global 2000 firms hailing from that country have known breaches. The Netherlands also sits above the US in second place with 22%. Canada and France round out the top five.

Checking in with the lowest relative breach rate is... China. But you might want to put those business relocation plans on hold—China's less-than-transparent regulatory and breach reporting regimes undoubtedly skew these stats. China is also known more as a source of cyber threats than a target of them. YMMV.

Moving on from the frequency side of breaches among the Global 2000, let's see what we can infer about the financial fallout from them.

ARE GLOBAL 2000 BREACHES MORE OR LESS COSTLY THAN FOR SMBS?

Yes...and no. To explain this apparent contradiction, we'll once again tap into the CISA-sponsored Information Risk Insights Study (IRIS). The figure below plots the distribution of reported financial losses from historical cyber events. Labels indicate what constitutes a typical and extreme loss for breaches affecting firms in each revenue tier.

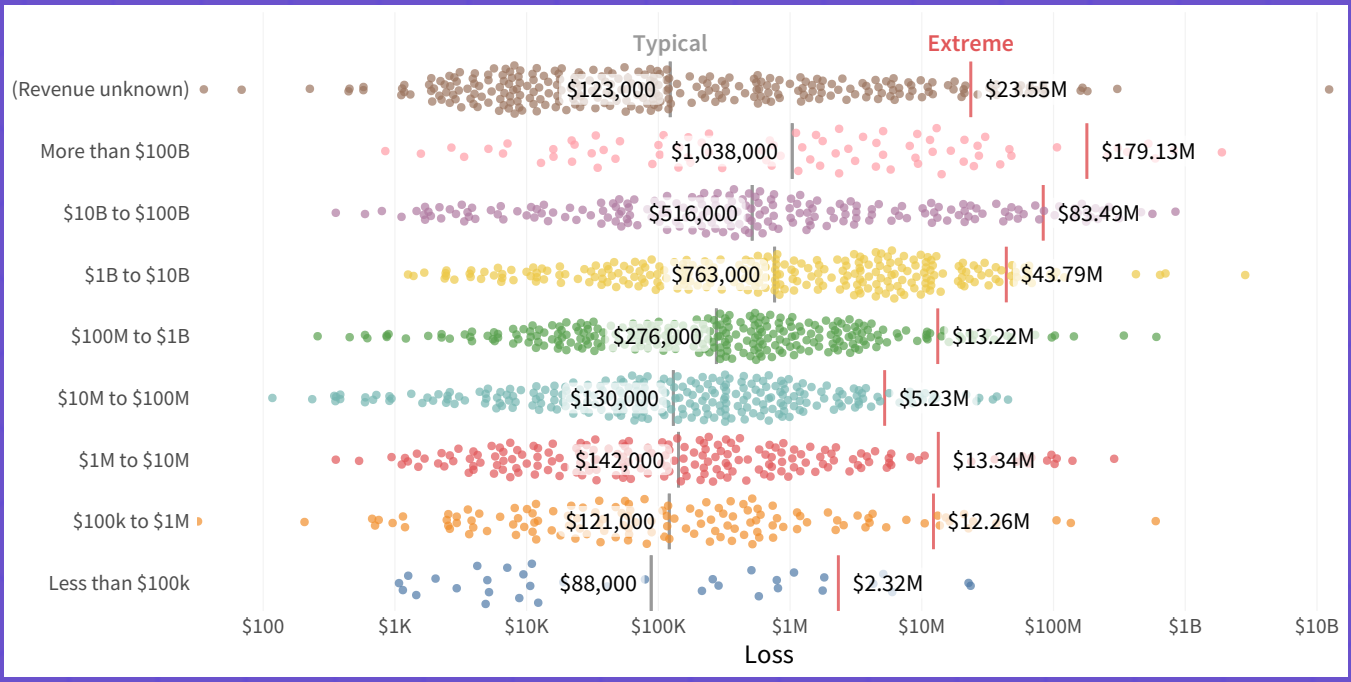


Figure 6: Distribution of reported cyber event losses by firm size (in revenue)

> *Breaches cost the largest companies ten times more on average, and extreme events are 77 times costlier!*

The absolute cost of an average breach for the largest companies is tenfold higher than that of their smallest counterparts. The delta for extreme events balloons to 77 times more! That's certainly worth considering when the Global 2000 conduct risk assessments.

The relative impact, however, tells a different story. A typical loss of $88K could well be a business-ending event for a small shop that brings in $100K annually. For a $100B enterprise, even an extreme loss upwards of $200M may not be considered a material loss.

What's the total cost of all these breaches experienced by the Global 2000 during this period? There's no sure way to answer that because the financial losses for most of them were never made public. That said, we can use what has been reported by the Global 2000 and other companies of similar sizes to project this (see the loss distribution in Figure 6).

ESTIMATED TOTAL LOSSES RANGE FROM $20 TO $80 BILLION, WITH POTENTIAL TO CLIMB TO SEVERAL HUNDRED BILLION.

Based on available historical data, we estimate total losses across all these events to be between $20 and $80 billion—though it could stretch as high as a few hundred billion. Why the large range? That's a reflection of the wide disparity in the reported costs of breaches. Financial losses are notoriously difficult to measure with precision and vary substantially based on a host of organizational and event-specific factors.

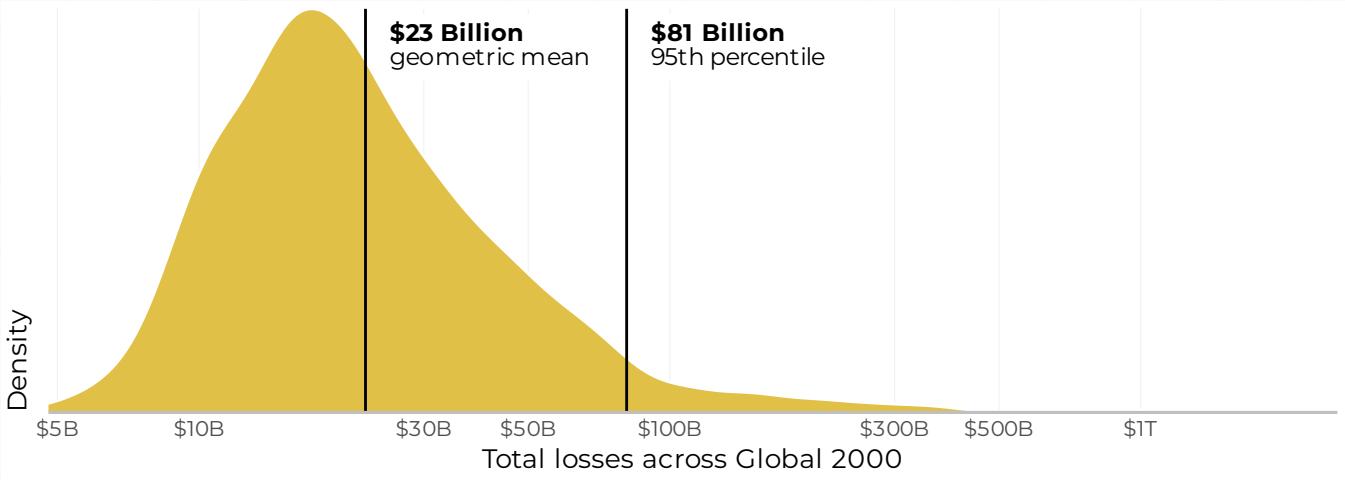


Figure 7: Estimated losses for recorded events in the Global 2000

Such significant losses would rank among the top 10 on the Global 2000 list by annual profits.

What we can infer with certainty is that these events represent a huge amount of destroyed capital across these companies. To put this into perspective, losses of this magnitude would rank in the top 10 on the Global 2000 list based on annual profits.

As impactful as that sounds, these first-party loss events are only part of the story of cyber risk across the Global 2000. There's also the aspect of third-party risk to consider. We'll do that in the next section.

Global 2000 Third-Party Ecosystem

We're working our way toward an analysis of breaches to third-party vendors of the Global 2000, but a short detour is in order before we get there. It would be helpful to have an understanding of the scope and security of these supplier relationships because that ecosystem defines the context for third-party risk. So, let's look into that now.

Our reconnaissance detects nearly 18,000 different technology and service products that are directly used by the Global 2000. Per Figure 8, the typical number of products used is 361, but about 20% of these companies use a thousand or more products. And keep in mind that this accounts only for those that are externally visible.

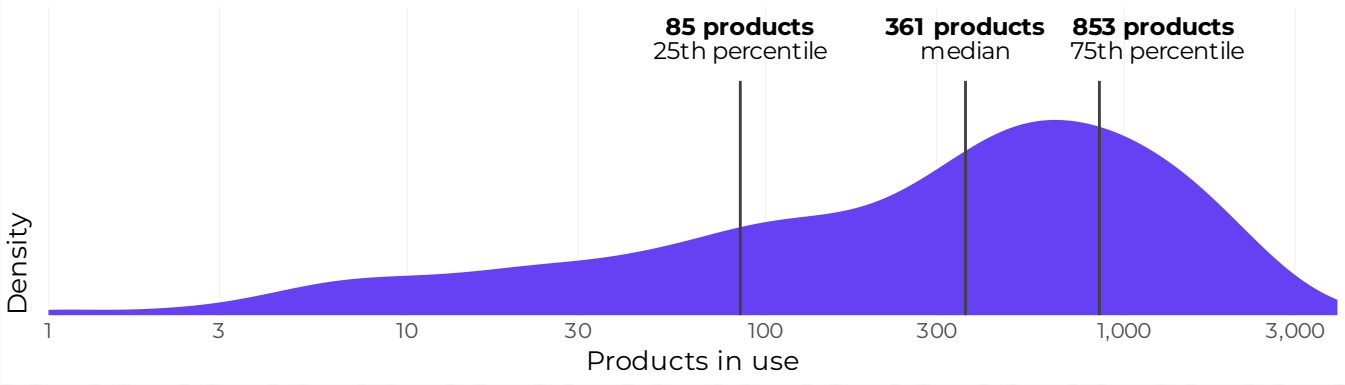


Figure 8: Products used by the Global 2000

Those products are supplied by over 8,000 different vendors. The median number of vendors used by the Global 2000 is 144, but that stretches beyond 1,000 for some of them (see Figure 9). Perhaps even more amazing, is that there's a subset of the Global 2000 with ties to fewer than 10 vendors.

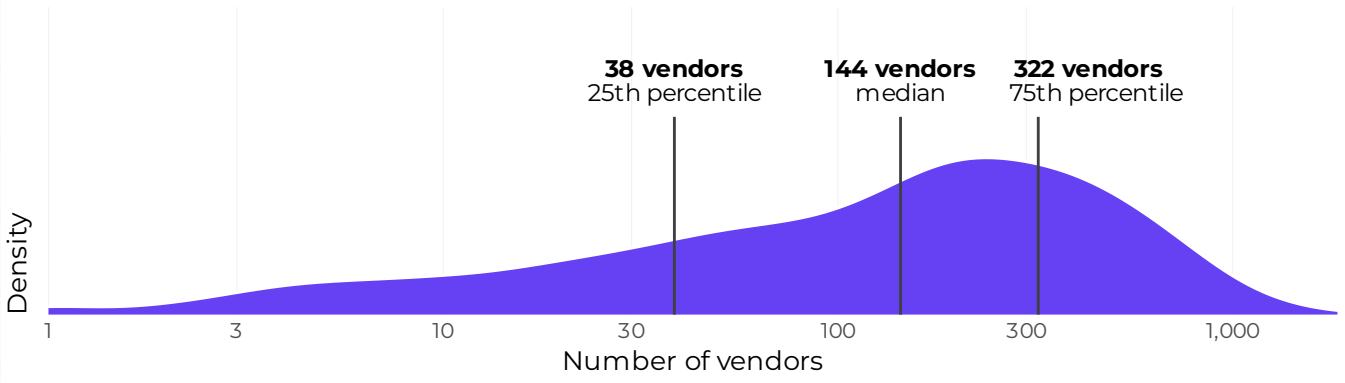


Figure 9: Vendors used by the Global 2000

What types of vendors and products are represented here? Figure 10 gives a general sense of that breakdown, and by and large, it's the kind of stuff you'd expect. Lots of enterprise application vendors (e.g., SAP and Oracle), data center solutions, digital marketing services of varying types, productivity solutions and other software, etc. We've included this for context when thinking about managing large tech footprints across many entities, but we'll remain at the vendor level.

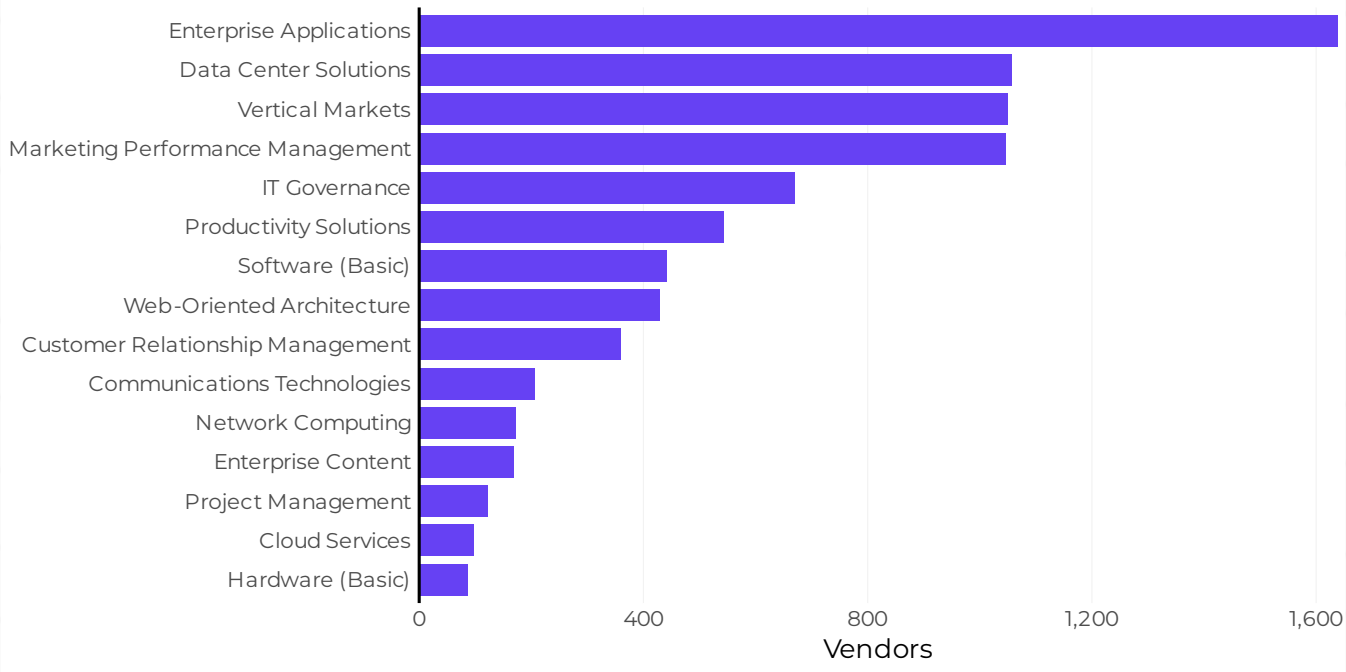


Figure 10: Types of vendors used by the Global 2000

THESE TECHS LOOK NORMAL—WHAT'S THE CONCERN?

That's a good observation; they are normal. And that's a big part of the issue because when technologies become normalized, our trust in them and dependency upon them grows. This opens the door to threats that exploit those conditions.

The recent supply chain attack targeting a very common JavaScript library, Pollyfill[.]io, offers a case in point. Pollyfill's purpose in life is to enable old browsers to support non-native functionalities. Nothing too scary there, right? But attackers saw the library as an opportunity to surreptitiously inject malicious code into hundreds of thousands of websites. It worked and impacted major companies around the world.

This library probably didn't sit high on anyone's riskiest software list, but it did land on attackers' radars as an ideal target. Managing the myriad mundane third-party libraries, open-source software, and IT services that organizations in the Global 2000 use every day is one of the biggest challenges for cybersecurity teams.

In general, there is a strong correlation between the size of companies, as measured by their market valuation, and the number of vendors they use. Mo' money, mo' partners (we'll see if that leads to mo' problems a bit later).

Within that broad trend, however, there is quite a bit of variability. Some of the smaller Global 2000 firms have abnormally large third-party networks and some of the biggest ones work with just a few vendors (what's up with that $300B org with <10 vendors?).

Figure II: Relationship between company market value and number of vendors used

Perhaps some of the variation seen in the former chart has something to do with the nature of the organization and its services? To investigate this, we'll use the chart below to explore the typical number of tech vendors for companies in each sector.

> *Mo' money, mo' partners: A strong correlation exists between company size, as measured by market valuation, and the number of vendors.*

It's an interesting list. We expect the Media & Internet and Telecommunications sectors to have expansive digital supply chains. But we don't expect Wholesale companies and Healthcare providers to be right up there with them. As described in our study, The Cyber Risk Landscape of the U.S. Healthcare Industry, the sector is incredibly diverse with digital footprints that often resemble those of IT and manufacturing firms.

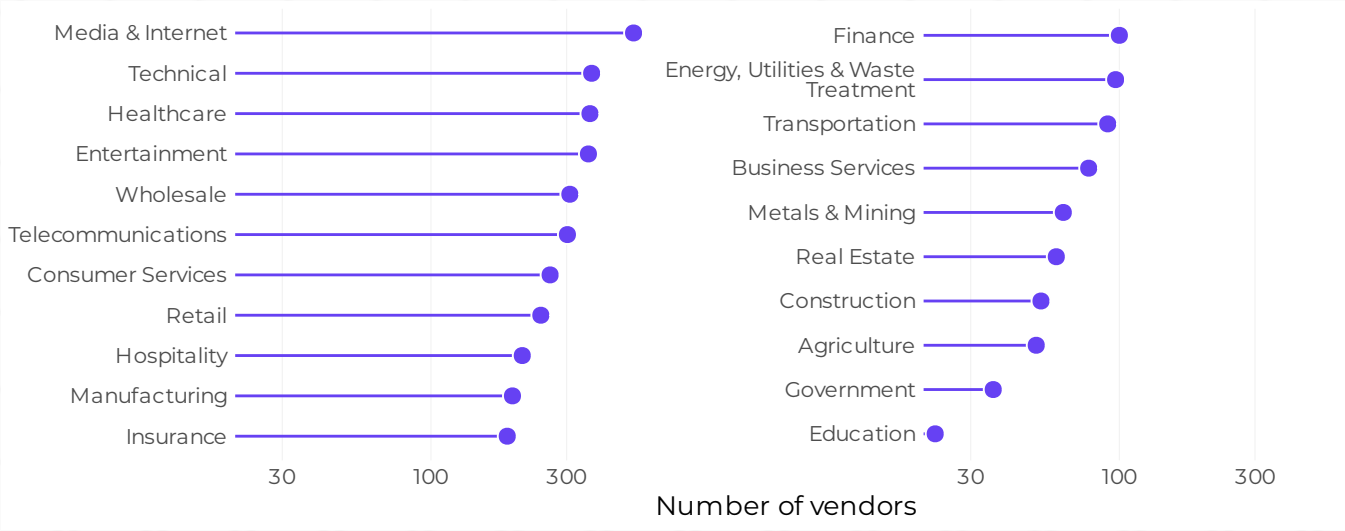


Figure 12: Median number of vendors per Global 2000 firm by industry

On the opposite end, the low number of vendors for Education may strike some as surprising. It did us, so we investigated a bit further. First, note that there are few companies in this sector large enough to make the Global 2000 list. Also keep in mind that what we show here does not include all the myriad tech owned by students running on those educational networks.

There also appears to be some variation in the size of third-party networks by country. North American and European countries dominate the left side of Figure 13 with the largest number of vendors. Asian representatives of the Global 2000 tend to have comparatively third-party relationships, but factors like the "Great Firewall of China" undoubtedly have an effect on visibility here.

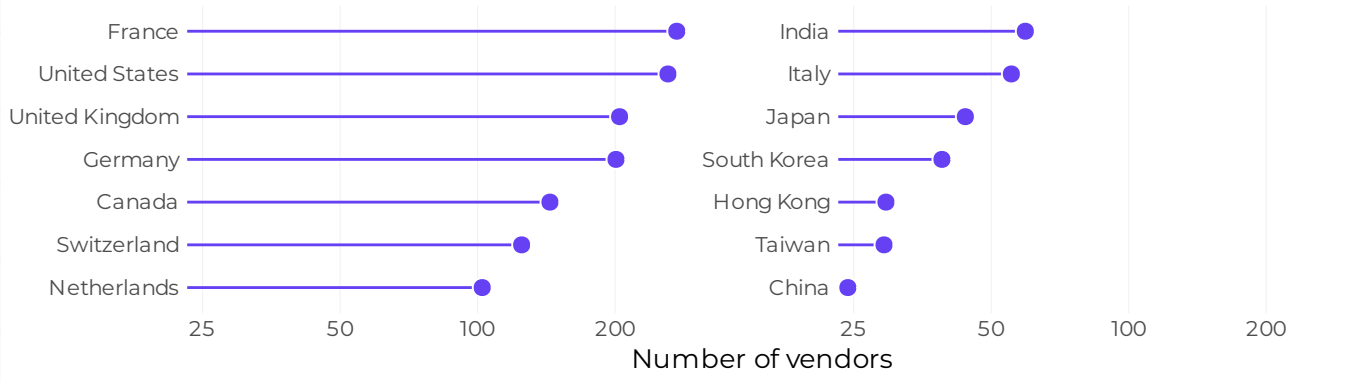


Figure 13: Median number of vendors per Global 2000 firm by country of origin

We've looked at the scope of the third-party ecosystem, but what about the security of these vendors? Are they better or worse than the Global 2000? Let's find out.

Similar to the Global 2000, the majority of their vendors earn pretty good marks from SecurityScorecard. Scores of A and B are the norm in Figure 14, but there are definitely some vendors that would raise concerns for Global 2000 third-party risk managers.

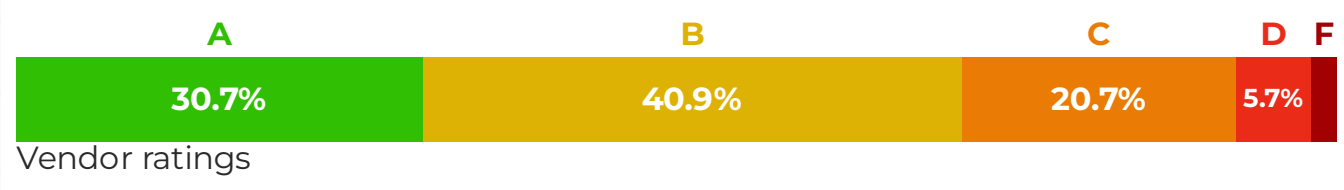


Figure 14: Distribution of SecurityScorecard ratings for vendors of the Global 2000

Since scrolling between Figure 2 (the Global 2000) and Figure 14 (the vendors) is rather tedious, we'll add a separate chart that provides a direct comparison of SecurityScorecard ratings between these two groups.

Think of Figure 15 below as a one–to–one comparison of all of Global 2000 companies (the first party) and all of their third-party vendors.

69% OF THE TIME, GLOBAL 2000 MEMBERS SURPASS THEIR VENDORS IN SECURITY RATINGS, WHEREAS THIRD PARTIES HAVE THE ADVANTAGE IN 28% OF THE RELATIONSHIPS.

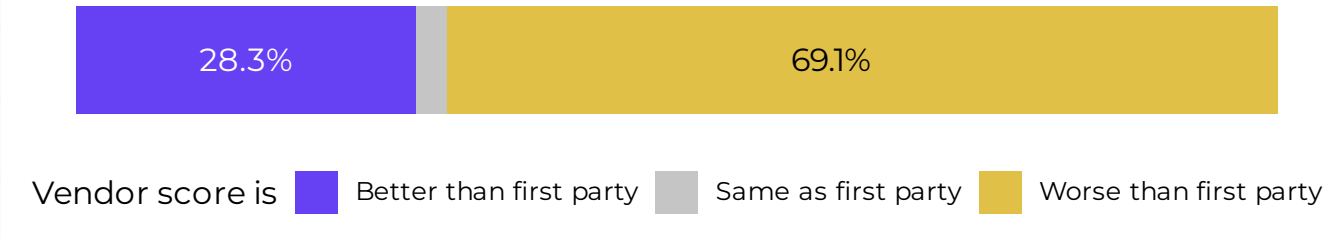


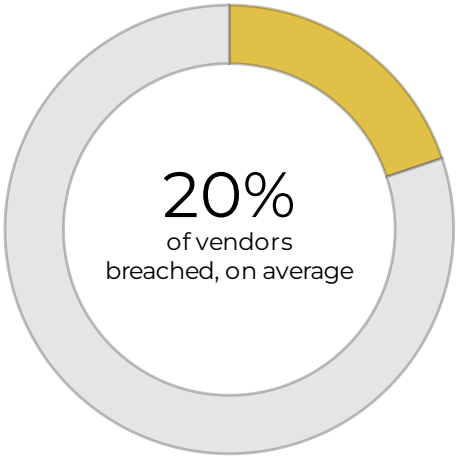
Figure 15: Relative SecurityScorecar ratings for the Global 2000 vs. their vendors

In the majority of cases (69%, to be exact), the Global 2000 member boasts a higher security rating than the vendor. Third parties have the upper hand in 28% of those relationships. There's a very small set of cases (<3%) where each part scores roughly the same.

All in all, this fits in with the common idea that megacorporations like those in the Global 2000 tend to have higher-than-average incentives, resources, and regulatory pressure to improve their security postures. That's a good thing because we're about to see that there's a thick cloud of third-party risk surrounding them.

Breaches in the Global 2000 Third-Party Ecosystem

The headline stat for this section has already been shared—99% of Global 2000 companies are connected to a third party that has suffered a known security breach in the last 15 months. But how does that translate across the large ecosystem of suppliers these organizations work with? Is there just one outlier in the group or are breaches the norm across them all?



As with many things, the truth is somewhere in between those extremes. There's usually more than one affected vendor, but it's rarely the whole bunch. On average, 20% of the third parties used by a Global 2000 company have suffered a recent breach. An unfortunate few have vendor breach rates as high as 50%, but lower percentages are far more common.

Figure 16: Proportion of vendors with a breach for each Global 2000 company

OK—one in five of your vendors is going through a breach (assuming you represent a Global 2000 company). How does that translate into absolute numbers? That's not too difficult to derive using a little math that essentially combines Figures 9 (number of vendors) and 16 (percent breached). Figure 17 shows the result.

WHILE BREACH RATES CAN PEAK AT 50%, AN AVERAGE OF 20% OF THIRD PARTIES SERVING GLOBAL 2000 FIRMS HAVE SUFFERED A RECENT BREACH

Less than 5% of the Global 2000 can claim that no more than one of their third parties have been breached. About 40% of them have somewhere between 2 and 20 breached vendors, and another 40%+ range between 21 and 50. The final 15% operate within third-party ecosystems that contain 50 or more vendors with known breaches.

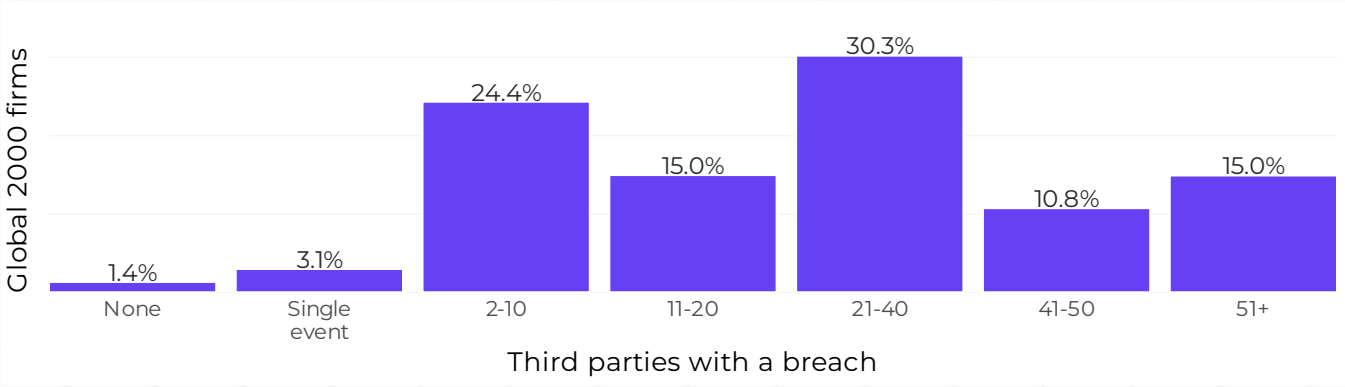


Figure 17: Number of third parties experiencing breaches

With a little more math, we can also estimate the probability of a given number of breaches across a Global 2000 company's network of suppliers over a 12-month period. It's not surprising that it's almost certain that they'll encounter at least one third-party breach. And there's a 75% chance of exposure to 10 or more. This leads naturally into a discussion of concentration risk.

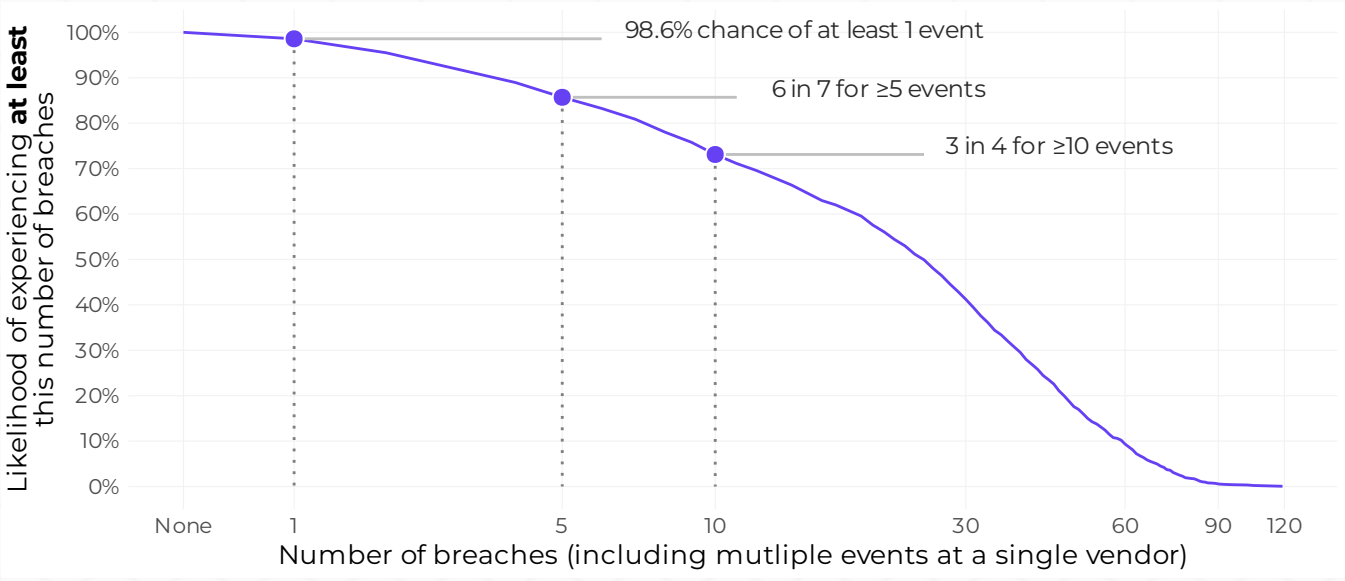


Figure 18: Probability of having at least a given number of third-party breaches

Concentration Risk Encircling the Global 2000

"An avalanche starts with one pebble." –Jay Kristoff, Endsinger

The very real prospect of multiple vendors in your digital supply chain experiencing breaches stokes concerns about the concentration of cyber risk. Concentration risk stems from the fact that our reliance on ubiquitous technologies creates massive single points of failure, which can trigger widespread impacts when these systems are disrupted or compromised. It's a risk that's especially relevant to the Global 2000.

Why? Well, for starters, the Global 2000 are a highly interconnected, interdependent group. Nine out of 10 of companies on the list provide products and services to other Global 2000 firms. In other words, they're vendors too. About 12% of all the third-party relationships analyzed in this report are between Global 2000 companies.

Figure 19: Interrelationships among Global 2000 companies

GLOBAL 2000 COMPANIES FACE SIGNIFICANT CYBER RISK DUE TO THEIR INTERDEPENDENCE, WITH 90% ACTING AS VENDORS TO EACH OTHER.

Another aspect of concentration risk for the Global 2000 to consider is that a few select vendors have a disproportionately huge scale of deployment across the ecosystem. Figure 20 puts some numbers behind that statement. Each of the eight most widely deployed vendors are used by at least 80% of Global 2000 companies! Circling back to the former point, six of those eight are themselves members of the Global 2000 elite.

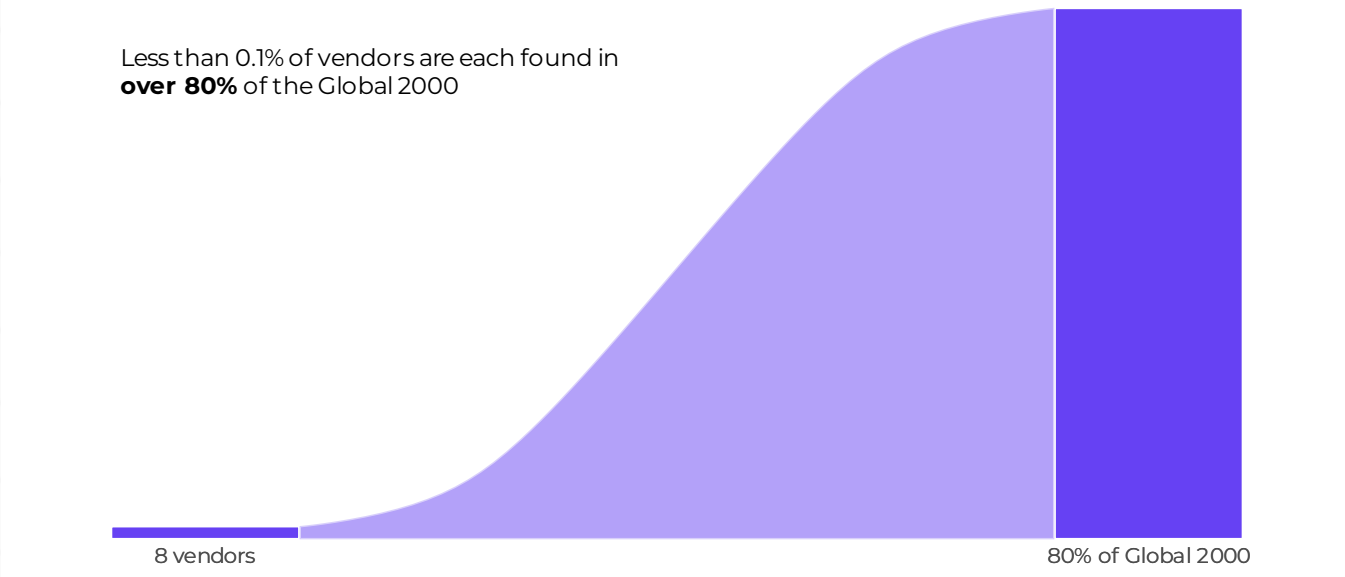


Figure 20: Percentage of vendors used by Global 2000

In an ideal world, the most widely used vendors would be the least susceptible to cyber attacks and security failures. Figure 21 makes it clear that we don't live in that world. In the real world, four of the top five suppliers of the Global 2000 have had a recent breach. Pushing that out a bit more gets us to 9 of the top 25 (36%) vendors. It's like the warning on your rearview mirror—"Breaches in this network are closer than they appear."

FOUR OF THE TOP FIVE GLOBAL 2000 SUPPLIERS HAVE FACED A RECENT BREACH.

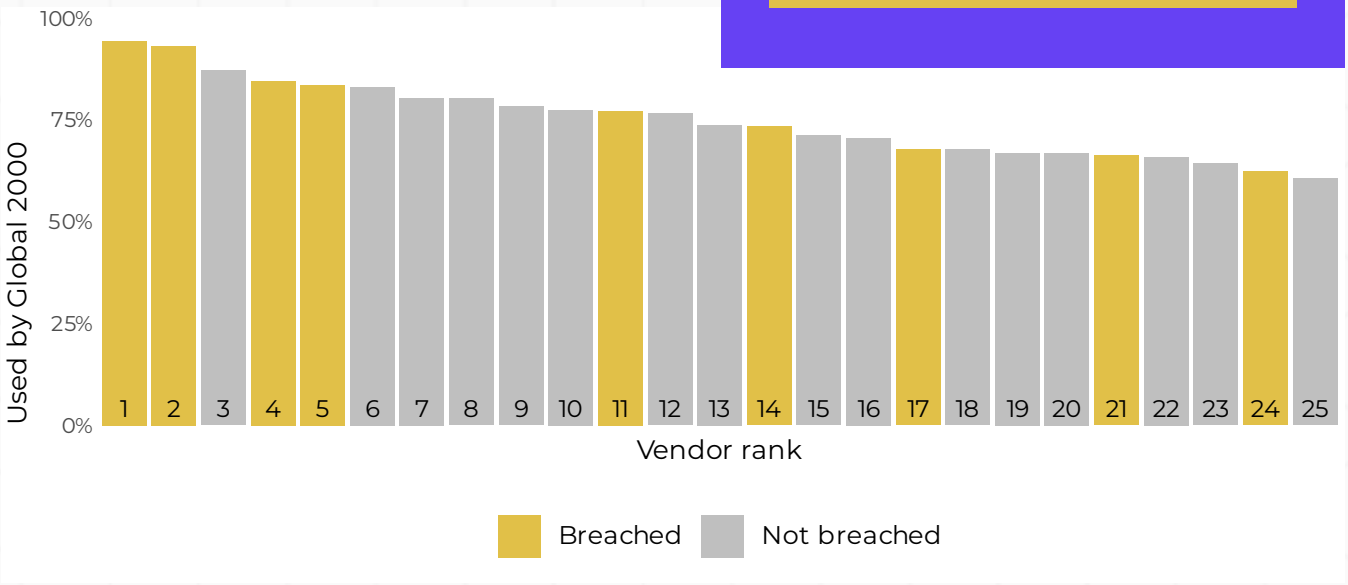


Figure 21: Breaches among the most widely-used vendors of the Global 2000

WHAT'S A REAL-WORLD EXAMPLE OF CONCENTRATION RISK?

As we were adding the finishing touches to this report, news broke of a massive global outage caused by a faulty update of CrowdStrike's Falcon endpoint security product. The event caused Microsoft Windows devices to crash, disrupting major operations across aviation, banking, healthcare, retail, and other sectors.

This incident is rather ironic, since organizations deploy CrowdStrike to protect against security events, not cause them. It's just the latest example of how routine updates of everyday products can have widespread impacts when things go wrong. It's also why Knowing Your Supply Chain (KYSC) is becoming an increasingly important component of cyber resilience.

This next figure is an attempt to consolidate what we've learned thus far about concentration risk across the Global 2000. The horizontal axis plots vendors based on their scale of adoption across the Global 2000. The vertical axis corresponds to the number of known breaches, with an emphasis on none (purple), one (yellow), and multiple (white) events.

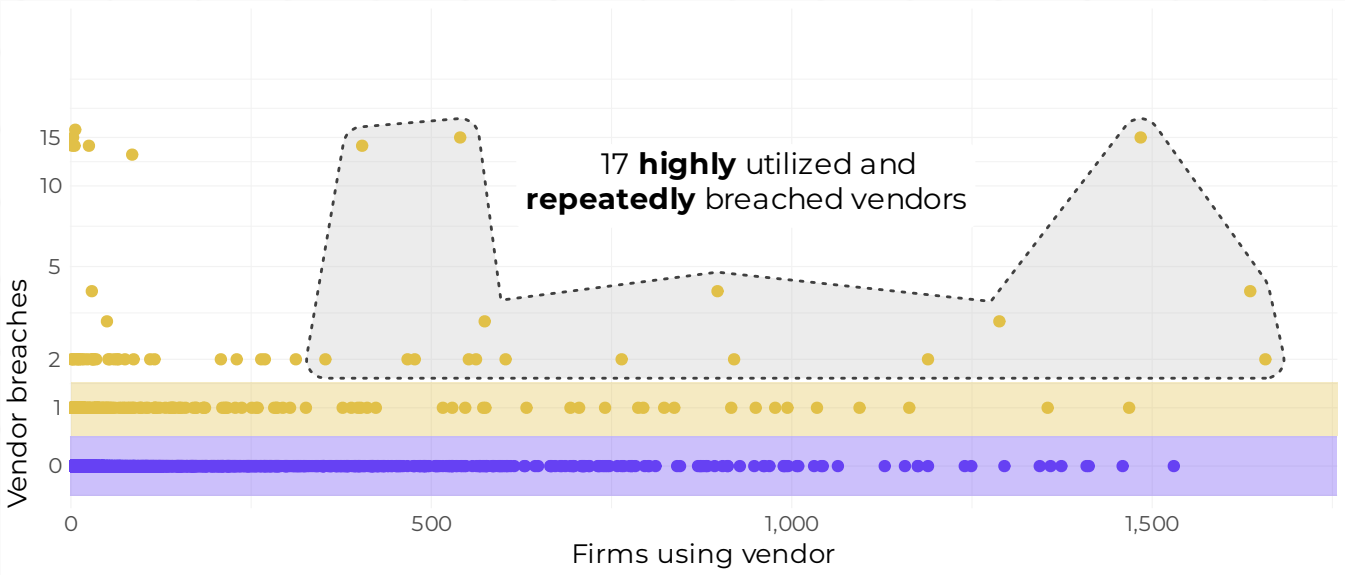


Figure 22: Firms using vendors vs. number of breaches in those vendors

The vendors within the gray shaded region exhibit the toxic combination of high adoption and multiple breaches. In other words, they're the most likely sources of concentration risk for the Global 2000. Want to know more about such companies and how to protect your supply chain? Check out our joint report with McKinsey & Company, Concentrated Cyber Risk in a Global Economy.

Multi-Party Events

One final facet of concentration risk we want to touch on in this report concerns multi-party security incidents. As the name implies, these are security events that involve multiple parties that share some form of business relationship.

When thinking of multi-party events, our minds often go to APT-style supply chain attacks that infiltrate an upstream party and worm their way into your environment. But it also includes scenarios involving insider threats, cloud provider outages, and breaches of data aggregators or custodians. The Pollyfill (malicious) and CrowdStrike (accidental) incidents mentioned in prior callouts are examples of the wide range of multi-party incidents.

> *Multi–Party Events: Security events that involve multiple parties that share some form of business relationship*

Such events thankfully don't happen constantly, but they're not rare either. "Steady drumbeat" comes to mind looking at the historical frequency of multi-party incidents in Figure 23. We know of 3 times as many of them over the last 10 years compared to the prior decade.

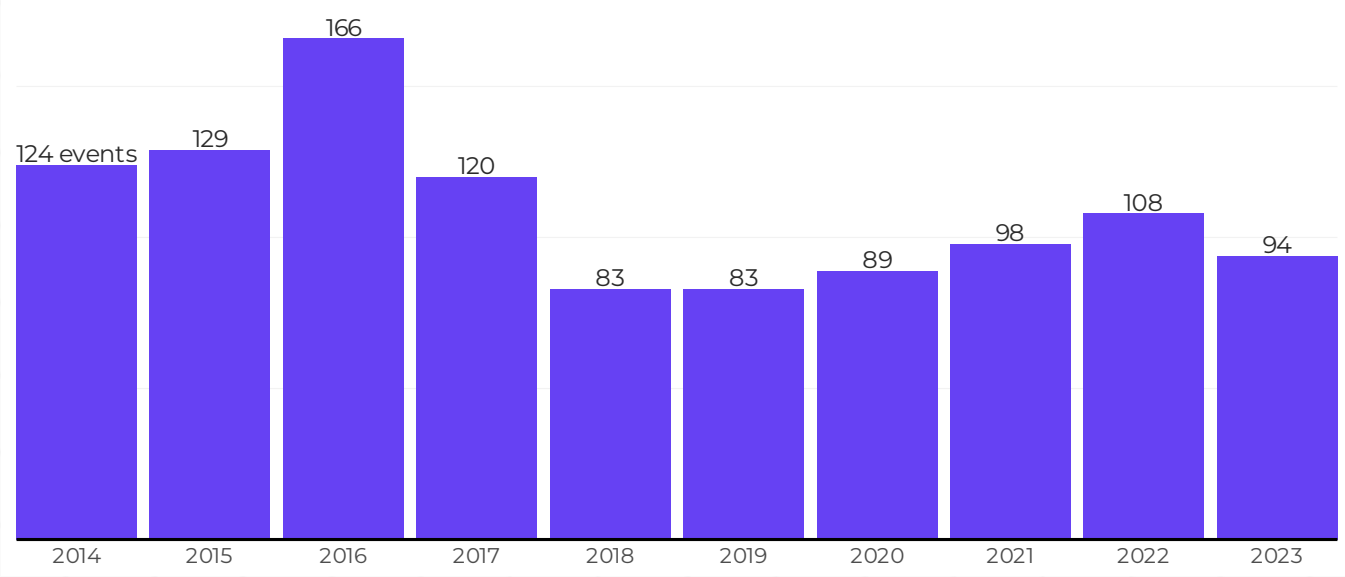
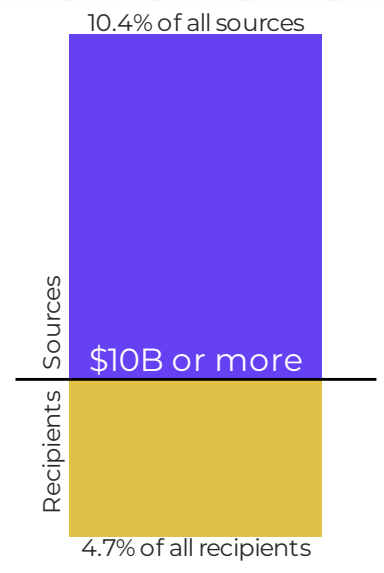


Figure 23: Frequency of multi-party security incidents each year

Can the impacts of these multi-party breaches spillover to the Global 2000 and/or their partners? You betcha—that's what makes mitigating multi-party incidents so challenging. While your organization may have strong security defenses in place, the actions of a third party can undermine those controls to cause harm anyway.

MULTI-PARTY EVENTS HAVE A MEDIAN LOSS 17 TIMES GREATER, WITH A SIGNIFICANTLY HIGHER RISK OF BILLION-DOLLAR LOSSES!



Among the Global 2000, however, things tend to go the other way. Member companies are twice as likely to be the source of multi-party incidents than the downstream recipients of them (Figure 24). That probably has a lot to do with their large stature and position at the top of the supply chain.

What about the financial impact of multi-party events? Perhaps they're not as costly as events that are absorbed by a single organization because losses are shared among all parties involved. Actually, it's quite the opposite. The financial losses are compounded as more organizations are impacted, not shared.

Figure 24: Global 2000 as a source vs. recipient of multi-party events

This can be seen in Figure 25. If we look at all types of security incidents (not just involving the Global 2000), the median loss magnitude is just south of $260,000 with only 5% exceeding $25 million. But the median loss for multi-party events is 17X higher with a much longer tail risk of billion-dollar loss events!

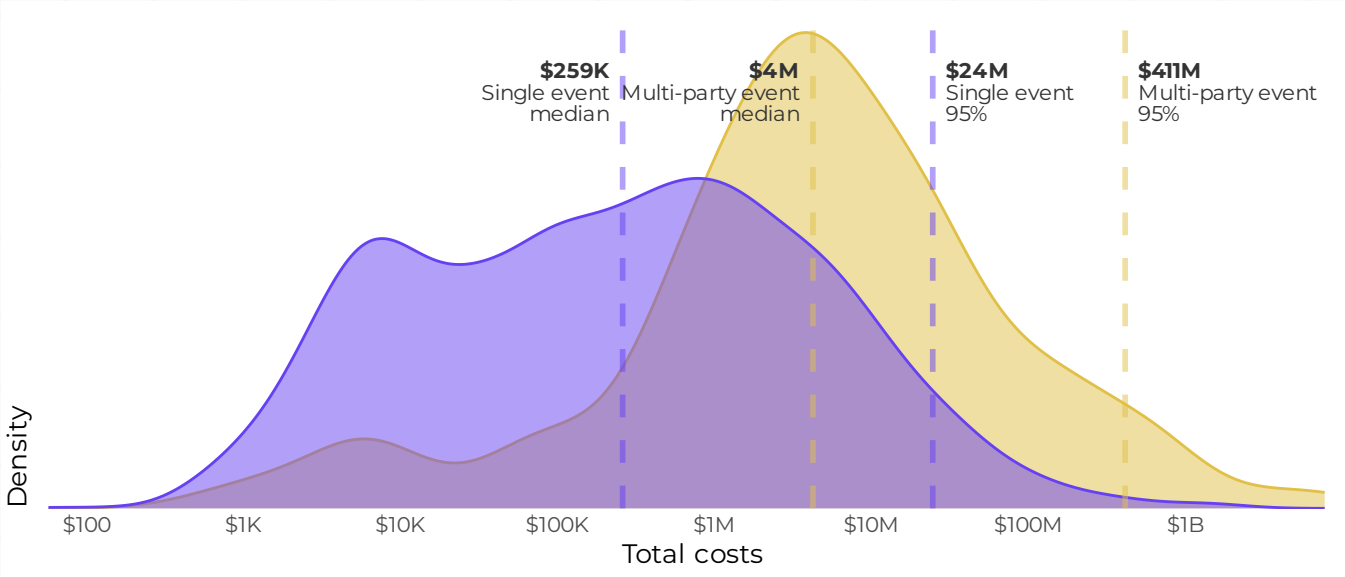


Figure 25: Comparison of single party and multiparty events

> *While the Global 2000 boasts $51.7 trillion in revenue, their interconnectedness exposes them to severe cyber risks, with 99% tied to breached vendors and possible losses up to $80 billion. Addressing this concentrated risk is vital for third-party risk management, and this report offers valuable analysis to assist in these efforts.*

By any of these measures, concentration risk is definitely something Global 2000 third-party risk management programs should be concentrating on. We hope the analysis shared in this report will help your team do exactly that.

Conclusion

Sun Tzu's "Know your enemy" advice might well be the most widely used quote in the field of cybersecurity. The next phrase of his quote often gets dropped, probably due to our industry's enthrallment with external adversaries: "...and know yourself."

Part of knowing yourself for an organization in the modern digital age is knowing your supply chain. This knowledge is increasingly important for cyber resilience, and understanding the dependencies within your organization and those of your vendors is critical to effectively manage risk. As this study has made abundantly clear, even the largest and most reliable organizations can experience issues.

To truly know your supply chain, questionnaires just won't cut it. Even if you could trust vendor responses to be accurate, obtaining that information once every few years offers little insight into where things stand now. SecurityScorecard's Automated Vendor Detection bypasses that issue by providing a current and comprehensive Software Bill of Materials (SBOM) for each company in your digital supply chain.

You can get started right away for free and/or request a demo from one of our experts. There's no quicker way to discover hidden risks across your Nth-party ecosystem!

About SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third- party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn. Gain continuous visibility into your digital footprint, vulnerabilities, and clear steps to remediate them with SecurityScorecard. Claim your free account and take control of your cybersecurity risk.

About The Cyentia Institute

The Cyentia Institute is a research and data science firm working to advance cybersecurity knowledge and practice. Cyentia pursues this goal through data-driven studies like this one and through a growing portfolio of analytic services. Learn more at www.cyentia.com.