THE TRUE IMPACT OF CONCENTRATION & CASCADING RISK

Learn more about the role concentration and cascading cyber risk play in your company and how to avoid the negative effects of a third-party cyber incident.

BLACK KITE

TABLE OF CONTENTS

Introduction to Concentration and Cascading Cyber Risk

Third-party cyber risk is the cyber risk organizations introduce into their digital ecosystem when they rely on third parties to help support their supply chain and produce their products and services.

When organizations think of this risk, they often focus their third-party risk management efforts on minimizing the effects of an attack. These attacks, after all, can wreak havoc on an organization:

- Breaches due to third-party software vulnerabilities cost companies an average of **$4.55 million per attack.**
- In a 2022 CyberRisk Alliance Resource survey, **8 out of 10 tech executives reported suffering from network outages** due to a third-party attack.

But let's back up. The focus shouldn't (just) be on mitigating the impact of breaches once they occur. Instead, organizations should look to understanding the concentration and cascading risk in their infrastructure and mitigating high-risk areas in their ecosystem.

Since concentration and cascading risk are types of third-party cyber risk, assessing and responding effectively to both should play an important role in your organization's third-party cyber risk management strategy.

Doing so will help your company reduce the negative impacts of third-party vendor breaches, and breaches that occur on the fourth- and fifth-party vendor levels.

Concentration and cascading risk affect nearly every part of your organization: from the software you choose to use to the vendors you work with.

In this eBook, we'll dive deep into concentration and cascading risk and how you can leverage both to protect your organization against overall third-party cyber risk.

WHAT DO WE MEAN BY "HIGH" RISK?

When we talk about high risk or exposure in concentration and cascading risk, we're referring to instances where the level of risk could critically impact your organization.

Since this differs across companies and industries, it's important to consider your company's unique infrastructure, business goals, and vulnerabilities when determining risk impact.

WHAT IS CONCENTRATION RISK?

What is Concentration Risk?

You may have heard of concentration risk before in the context of banking and your investment portfolio. The meaning, however, translates to third-party cyber risk management. **Concentration risk is the level of risk an organization faces due to the concentration of value or assets in a single entity.**

For example, your concentration risk may be high if your retail company depends on a single point of sale (POS) system. If the POS company is compromised and unable to provide service, the disruption to your retail company's business processes would be considerable. In contrast, you might have low concentration risk if your retail company depends on a single third-party vendor to supply packing boxes. While it would inconvenience your company if the box supplier was compromised and unable to provide the goods you need, you'd still be able to find suppliers with readily available inventory.

Thinking about concentration risk in your organization helps you determine where you may be relying too heavily on a single vendor to provide an asset or service. It also enables you to consider how your company would be affected should that vendor become compromised and unable to deliver that asset/service you rely on.

Every organization has some concentration risk: It's nearly impossible to eliminate. To eliminate concentration risk, an organization would have to partner with multiple vendors for each asset and service in their ecosystem.

Returning to our retail company example, your organization would need backup POS systems, shipping service providers, inventory software options, and more. Duplication like this is expensive, time-consuming, and impractical. Most importantly, there's no such thing as a completely secure vendor.

Instead, your TPRM strategy should focus on accurately assessing concentration risk throughout your organization. Then, based on the amount of risk in a particular area, you'd take the appropriate steps to lower or mitigate the risk.

TO DETERMINE YOUR ORGANIZATION'S CONCENTRATION RISK, WE RECOMMEND ASKING THE FOLLOWING QUESTION:

"Have we concentrated a particular critical service on a single vendor, creating a single point of failure?"

It can also be helpful to picture your organization and its ecosystems like a map or interconnected web.

"How many connections are broken, removed, or negatively impacted if you remove one of the nodes on your web?"

Examples of concentration risk by context:

Concentration risk looks different across companies. It's important to contextualize a product's or service's significance to your organization when evaluating the level of risk. For example, purchasing office supplies (e.g., pens, pencils, and paper) from a single vendor in a digital office poses a relatively low concentration risk.

If that vendor is compromised, your organization may have to look elsewhere for office supplies, but it won't cause a significant business disruption.

Why? You can easily find office supplies from other vendors, and delayed access to office supplies may cause frustration/annoyance but not a significant disruption in the business.

However, suppose your company still relies on hard copies and other non-digital business elements. In that case, your office supply vendor poses a high concentration risk, as you rely on the vendor for essential business supplies that impact your day-to-day work operations. When that vendor is compromised, your organization could experience business disruption (e.g., the inability to generate forms, store physical data, etc.).

Examples of high concentration risk by industry:

In addition to contextualizing a product or service's significance across (hypothetical) organizations to understand concentration risk, it can be helpful to consider what high concentration risk looks like across industries. Here are a few examples:

- **Retail:** A store relying on a single, third-party vendor like PayPal or Stripe to process payments would pose a high concentration risk. If the third-party payment vendor is compromised, the store may be unable to process customer payments.
- **Customer service:** An organization relying on a single customer service call center faces a high concentration risk scenario. In utilizing a single call center, this company would find itself both limited in the service it can provide (only able to assist clients during its hours of operation) and at risk for business disruption if compromised.
- **Manufacturing:** Relying on a single, third-party vendor at any point of its supply chain would create a high concentration risk situation for the manufacturing organization. Whether the company is dependent upon a single vendor to provide the raw materials needed for the final product or the shipping services at the end of the supply chain, this organization is setting itself up for significant disruption if the third-party vendor is compromised and unable to provide the materials/services.

When assessing the concentration risk posed by your vendors, you must consider and prioritize the factors unique to your organization (e.g., how your company uses the product/service provided by the third-party vendor). Considering those factors ensures that the level of risk you're assigning to an asset or service is accurate.

WHAT IS CASCADING RISK?

What is Cascading Risk?

Have you seen those videos where someone spends hours setting up dominos and, with a tiny push, sets off a chain reaction that reveals a spectacular design? That's a perfect illustration of cascading risk. Cascading risk is the domino effect that occurs when a single vendor is compromised, and their exposure leads to increased risk, exposure, and vulnerability for their connected vendors.

Considering your organization's cascading risk is crucial as businesses are more interconnected than ever. While you partner with a third-party vendor, that vendor also partners with additional vendors. The fourth-party vendor who provides assets and services to your third-party vendor may indirectly access your information.

Additionally, if your third-party vendor's vendor (fourth-party vendor to you) is compromised, the business disruption your third-party vendor experiences could considerably impact its ability to provide a particular service or asset that your organization depends on.

Similar to concentration risk, you can't completely eliminate cascading risk. To do so would require ending all of your organization's third-party vendor partnerships! Instead, you can assess and contextualize your cascading risk to effectively lower and manage your overall risk.

TO DETERMINE YOUR LEVEL OF CASCADING RISK, YOU SHOULD ASK TWO QUESTIONS.

The first question is: **In what ways am I connected to a particular vendor?**

Asking this helps you discover how your organization could be affected should a third-party vendor be compromised. For example, sharing information with a high-risk, third-party vendor can put you at risk for a data breach in the case of an attack. The at-risk data could include more innocuous data like your client's email addresses to personal identifiable information (PII).

The second question to ask yourself: **What is my proximity to this vendor?**

This question can help you determine the severity of impact to your organization should one of your vendors be compromised. Suppose you're sharing information with a third-party vendor, and the vendor shares that information with one of their third-party vendors. How would your organization be affected if a breach affected the fourth-party vendor's data?

Examples of cascading risk:

Due to the interconnectedness of modern organizations, no company is free from cascading risk. Let's look at a few additional examples of how different industries might classify cascading risk levels:

- **High Exposure:** An IT/software company's cloud infrastructure vendor falls victim to a ransomware attack. Considering the organization's connection to the vendor (most likely sharing data and dependent upon them for a critical service in their infrastructure), and the proximity (third-party, not fourth or fifth), the impact would be high.

- **Moderate Exposure:** A healthcare organization using a third-party medical billing company discovers the billing company's software provider is compromised. Depending on the amount of data shared with the billing company's software provider, as a fourth-party vendor to the healthcare organization, this may only present a moderate cascading risk.

- **Small Exposure:** An aerospace organization working closely with federal government agencies for permits and compliance requirements finds that one of the agencies was the victim of a cybersecurity attack. While the proximity is close, the risk level may be low due to the nature of the aerospace organization's connection to the government agency. Outside of permit and compliance information, the government organization may have little additional information on the aerospace organization. This lack of information reduces overall vulnerability should an attack occur, though the organization may experience some business disruption if the government agency cannot issue permits promptly.

THE COSTS OF HIGH CONCENTRATION AND CASCADING RISK

The Costs of High Concentration and Cascading Risk

Business disruption is possible for organizations whose third-party vendors experience a significant breach. Whether the business disruption results from high cascading risk, concentration risk, or both, it can cost your organization. Here is what could happen if you don't take action to identify and address unacceptable levels of concentration and cascading risk in your company:

COSTLY SUPPLY CHAIN DISRUPTION

When it comes to supply chain disruption, no person (or company) is an island. Most industries providing goods and services rely on a supply chain of sorts to do so. The cost of disruption to supply chains can vary depending on the industry, but here are a few averages:

- **Manufacturing:** the average supply chain disruption costs $610,000.
- **Automotive:** the average supply chain disruption costs $2.5 million.
- **Retail:** the average supply chain disruption costs $1.5 million.

These figures represent more than just the lost revenue companies experience when dealing with supply chain disruption. They also include the long-term impact on a company's competitiveness in the marketplace and the costs associated with reputational damage and loss of customer trust.

EXPENSIVE NETWORK OUTAGES

Companies facing high concentration and cascading risk may experience network outages if a vendor is compromised. When dealing with high concentration risk, an organization may have a single vendor providing its network services or servicing a large portion of elements in its infrastructure. If compromised, the business disruption the vendor experiences could cause outages in the client company's network. Whether concentration or cascading risk is the cause of a network outage, the cost is high: Gartner estimates unplanned downtime costs approximately $5,600 per minute.

The Costs of High Concentration and Cascading Risk

NON-FINANCIAL (BUT STILL FINANCIAL) COSTS OF BUSINESS DISRUPTION

The costs associated with high concentration and cascading risk go beyond the loss of revenue. If a company's vendor is compromised, the ripple effects can negatively impact that organization's reputation and market position. While these can also translate to loss of income, it's worthwhile to investigate these separately.

- Customer satisfaction and reputation: According to Zendesk, 95% of customers share a poor customer experience with others. Failing to deliver services and products on time, whether it's due to a concentration or cascading risk, can negatively impact a company's overall customer satisfaction rates, which in turn affects revenue.

- Market competitiveness: Companies that fail to address high concentration and cascading risk may fall behind in the market as they work to correct the damage caused by either risk. For example, a banking organization looking to launch new functionality in its mobile app (and attract new business) may shelve that upgrade if its only mobile app developer experiences a ransomware attack.

While the impact of high concentration risk and cascading risk is clear, organizations often need help managing and mitigating these types of risk effectively. Developing a strong third-party cyber risk management (TPRM) strategy is the answer. What this looks like depends on variables like your organization's security and business goals and contextualized risk. Let's explore some ways to get started with TPRM.

MANAGING YOUR ORGANIZATION'S CONCENTRATION AND CASCADING RISK

Managing Your Organization’s Concentration and Cascading Risk

When an organization considers just how heavily it relies on a single third-party vendor or follows the rabbit trails of vendor connections (fifth-, sixth-, and seventh-party risk), the prospect of risk mitigation can seem overwhelming.

However, an organization can take practical steps to reduce their exposure to risk or the severity of impact should a breach compromise their systems due to cascading or concentration risk.

FOCUS ON VISIBILITY

You have to understand your ecosystem before you can protect it. Visibility is more than just a headcount of your infrastructure’s elements, endpoints, and devices. Instead, it’s a holistic understanding of how those elements interact with each other, how they interact with their service providers and third-party vendors (including the data shared), and their influence across your organization.

Increased visibility enables you to identify areas of concern effectively. Perhaps you've stumbled across a point in your supply chain where you rely on a single vendor or discovered a third-party partner distantly connected to a much larger vendor experiencing a cybersecurity breach. Depending on your organization's acceptable risk level in these situations, you may not make any changes immediately. However, you will be able to monitor the situation and respond accordingly should the risk level change.

MEASURE RISK

Once you have a holistic understanding of your infrastructure and greater visibility into how the elements interact with each other, you can begin to prioritize your third-party vendors that pose the most risk and address them accordingly.

1) **Prioritize by proximity** for cascading risk: *An organization’s proximity to the attacked vendor dictates the impact of cascading risk*. With this in mind, your organization should catalog vendors and create a risk index that reflects the partner’s importance to your organization's business operations.

For example, a third-vendor connection directly influencing your organization's IT operations would rank much higher in risk than a fifth-party vendor distantly connected to your company's payroll operations.

Managing Your Organization’s Concentration and Cascading Risk

2) **Prioritize by the severity of impact** for concentration risk: *An organization can contextualize concentration risk by considering where they have vendors that pose an unacceptable level of concentration risk for their business.* It’s the difference between a concentrated risk in your office supply provider and a concentrated risk in your customer service support vendor.

Prioritizing risk can help you focus your mitigation efforts. Some risks may not require any action, while others may require immediate attention to ensure that your organization doesn’t experience the negative impacts of high concentration or cascading risk.

LEVERAGE THE RIGHT TOOLS

Gaining visibility into your ecosystem and prioritizing risk are huge undertakings. Both require significant research into your third-party vendor partnerships, ongoing monitoring of your vendors’ security positions and the threat landscape, and an understanding of your organization’s vulnerabilities.

Most companies don’t have the time and resources to complete this in-depth research. Instead, it’s best to leverage tools that can help you automate the visibility and monitoring process.

When searching for tools, you’ll also want to look for solutions that help contextualize the concentration and cascading risks you find. There are a variety of TPRM tools on the market, so you’ll want to focus on finding tools that provide intuitive, easy-to-understand feedback around you and your vendors’ risk levels.

Concentration and Cascading Risk Aren't Going Anywhere (and that's okay)

It's important to remember that there's no such thing as "zero risk." When it comes to cascading and concentration risk, as long as you have third-party vendors in your cyber ecosystem, both types of risk will be present, and you'll always be uncertain about the extent.

So in lieu of saying "adios" to all of your vendors or spending a ridiculous amount of time creating redundancies in your third-party vendor network, you can improve your TPRM strategy around these risks and help reduce the uncertainty.

While taking the appropriate steps to effectively understand your organization's levels of concentration and cascading risk is a good start, you'll also need the tools to prioritize and reduce these risks.

Building out your TPRM toolkit with solutions that help contextualize and mitigate the effects of high concentration and cascading risk puts you one step ahead of the game when it comes to strengthening your company's security posture.

Ready to start reducing your organization's concentration and cascading risk?

START WITH A FREE BLACK KITE RISK ASSESSMENT

ABOUT BLACK KITE

Black Kite is disrupting third-party risk management practices by providing security experts with the industry's most accurate and comprehensive cyber intelligence, resulting in unparalleled visibility into the risk vendors introduce into their environments.

The award-winning platform pushes the limits on predictive insights, delivering the highest quality intelligence to help organizations make better risk decisions and improve the health and safety of the entire planet's cyber ecosystem.

CONTACT US

✉ info@blackkite.com

📍 800 Boylston Street, Suite 2905
Boston, MA 02199

🌐 www.blackkite.com