BLACK KITE

KEY STATS

2025 THIRD-PARTY BREACH REPORT

After analyzing major incidents and patterns in last year's threat landscape, one big trend became clear:

Unnoticed vulnerabilities within third-party networks are exposing the fragility of online ecosystems.

BAD ACTORS LEVERAGED THIRD-PARTY VECTORS

In 2024, we saw bad actors stick to many tried and true attack vectors to cause incidents that rippled through diverse industries and ecosystems:

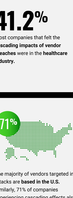
51.7%

Unauthorized network access remains a pervasive issue, accounting for half of publicly disclosed incidents (with many details remaining unknown).

56%

Compared to previous years, 2024 saw an estimated 56% increase in zero-day vulnerabilities. **Credential misuse** and **delayed vulnerability patching** were significant challenges for third-party systems.

66.7%



Ransomware was the second most common attack vector, accounting for two-thirds of all known attack methods. Third-party vectors were central to many ransomware campaigns.

THE MOST COMMON TARGETS FOR ATTACK WERE RICH IN SENSITIVE DATA

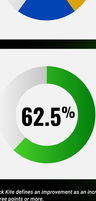
Bad actors still have their sights set on industries and companies rich in sensitive data. However, many incidents caused disruptions that spanned industries and geographies.

26%

Software services was the predominant source for breaches in 2024 and saw a significant increase from 2023.

41.2%

Most companies that felt the **cascading impacts of vendor breaches** were in the **healthcare industry.**



55%

71%

The majority of vendors targeted in attacks are **based in the U.S.** Similarly, 71% of companies experiencing cascading effects also are based in the U.S.

THE MOST NOTABLE INCIDENTS MADE MAINSTREAM HEADLINES

Many of 2024's most noteworthy cyber incidents made mainstream headlines due to their widespread impact on companies and consumers. Here are three examples:

CrowdStrike Outage:

This service outage impacted 8.5 million devices globally and caused an estimated $5 billion in direct costs and lost productivity.

Cencora Ransomware Attack:

This ransomware attack included what's estimated to be the largest ransom payment request in history: $75 million.

Snowflake Incident:

After bad actors breached Snowflake, they quickly gained access to giants like Ticketmaster, AT&T, Santander Bank, and LendingTree.

MANY INDUSTRIES ARE FIGHTING BACK

Amidst the challenges of 2024, many organizations fought back to mitigate risks and enhance their resilience. Here's what happened in the aftermath of many attacks:

20% software services
20% healthcare
20% finance

Of vendors that improved their cyber ratings* following a breach, 20% were in software services, 20% in healthcare, and 20% in finance.

62.5%

A majority of healthcare vendors improved their cybersecurity posture following an incident—the most of any industry. This may be due to regulatory requirements from frameworks like HIPAA.

**Black Kite defines an improvement as an increase in Cyber Ratings of three points or more.*

WHAT WE CAN LEARN FOR 2025

Despite the challenges of 2024, critical lessons emerged, revealing pathways to resilience and improved cybersecurity practices. Here's how security professionals can protect their companies from third-party breaches in 2025:

1. Enhance vendor cybersecurity practices
2. Implement proactive monitoring
3. Prioritize cross-industry collaboration

DIG INTO THE FULL REPORT

Read more about our biggest takeaways and specific recommendations on how your organization can build resilience by reading our full report, 2025 Third-Party Breach Report, The Silent Breach: How Third Parties Became the Biggest Cyber Threat in 2024 (no download required).

READ NOW >