BLACK KITE

2022 THIRD-PARTY BREACH REPORT

Trends, Root Causes and Lessons Learned from 2021

TABLE OF CONTENTS

INTRODUCTION

Today's imminent security threat is **connected risk.** In this annual report, the Black Kite Research team examined the impact of third-party breaches that occurred in 2021. The focus remains on understanding emerging vulnerabilities seized by cybercriminals, as well as target industries falling victim to breaches, stemming from a lack of due diligence.

While many of the hacker techniques have remained steadfast over the last few years, threats continue to evolve with new targets and smarter tactics.

Our goal at Black Kite is to make sure you gain awareness of what is most relevant in the threat landscape going into the new year.

Black Kite Research analyzed 81 individual third-party incidents, which ultimately lead to more than **200 publicly-disclosed headline breaches** and thousands of other inherent ripple-effect breaches throughout 2021. We studied why certain industry sectors faced higher susceptibility to an attack, as well as the most vulnerable vendors to the initial breach themselves.

Additional predictive intelligence on a subset of 63 vendors shows how an organization's **cyber posture improved when motivated to monitor** and deploy security measures. In turn, those without appropriate third-party risk management programs and policies in place became casualties to some of the most notorious breaches in history.

KEY FINDINGS

- **Ransomware became the most common attack method** of third-party attacks, initiating 27% of breaches analyzed in 2021.
- **Software publishers were the most common source of third-party breaches** for a third consecutive year, accounting for 23% of related incidents.
- **The average time between an attack and the disclosure date was 75 days**.
- The **healthcare industry was the most common victim** of attacks caused by third parties, accounting for 33% of incidents in 2021.

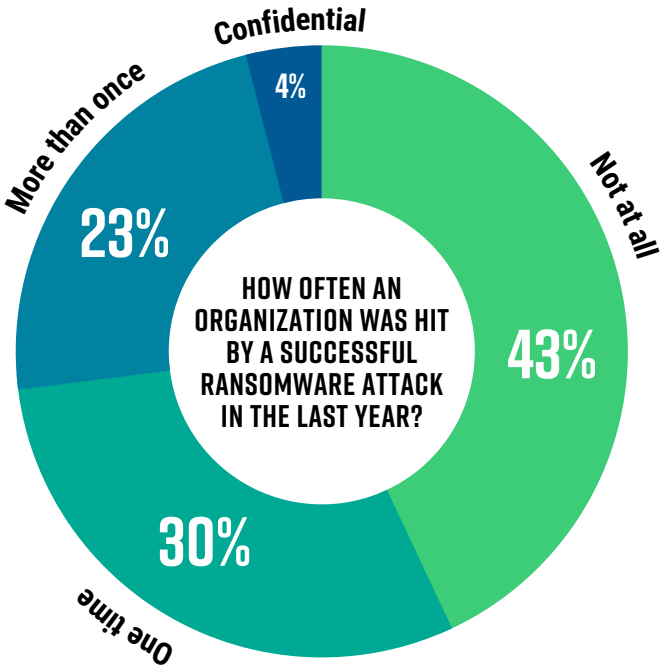
THE EVOLUTION OF THIRD-PARTY DATA BREACHES

With only a steady increase between 2019 and 2020, the number of third-party data breaches jumped 17% in 2021. What's behind the surge?

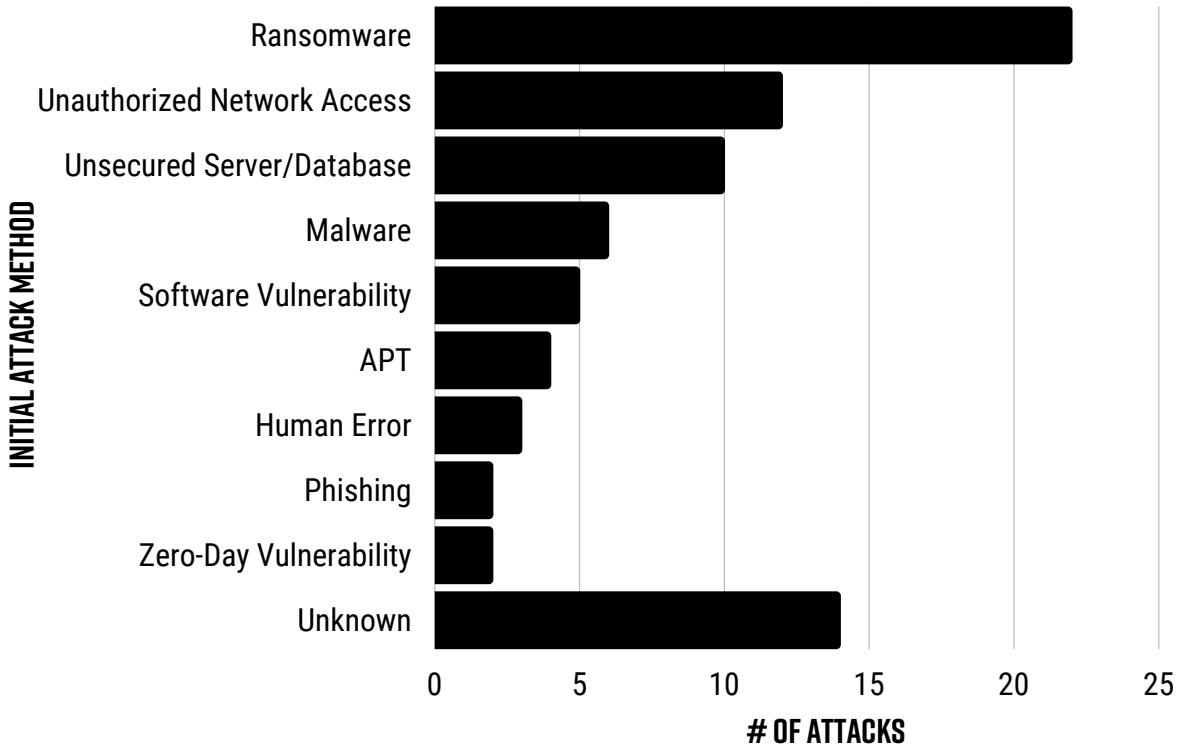
I. THE MOST EFFICIENT ATTACK METHOD

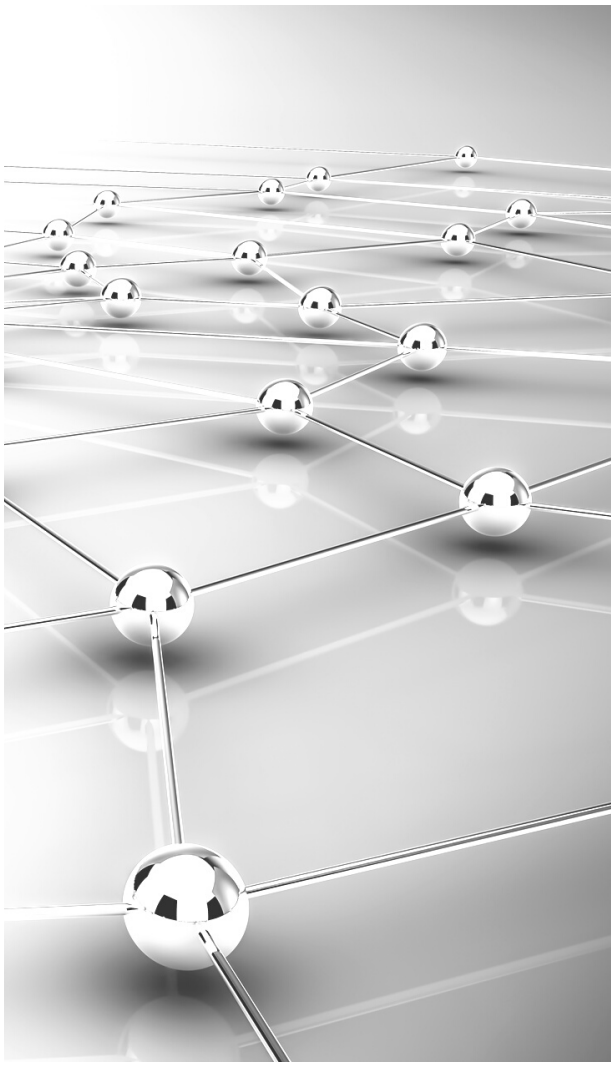
Accounting for only 15% of related attacks in 2020, in 2021, **ransomware** emerged as the **most common attack method** of third-party related breaches—accounting for **27%** of attacks. Ransomware is an extremely efficient attack approach, allowing data to be monetized quickly and easily.

In a Black Kite-sponsored report that collected feedback from 250 CISOs in 2021[1], 53% claimed they were hit at least once by a ransomware attack last year, with 69% expecting to face at least one ransomware attack in 2022.



ATTACK METHODS OF THIRD-PARTY BREACHES IN 2021





Unauthorized network access followed ransomware, contributing to **15% of breaches.** This method usually involves leveraging or cracking weak passwords and taking advantage of any vulnerabilities present in access control. Often, companies that do not want to disclose the details of an attack usually blame unauthorized network access.

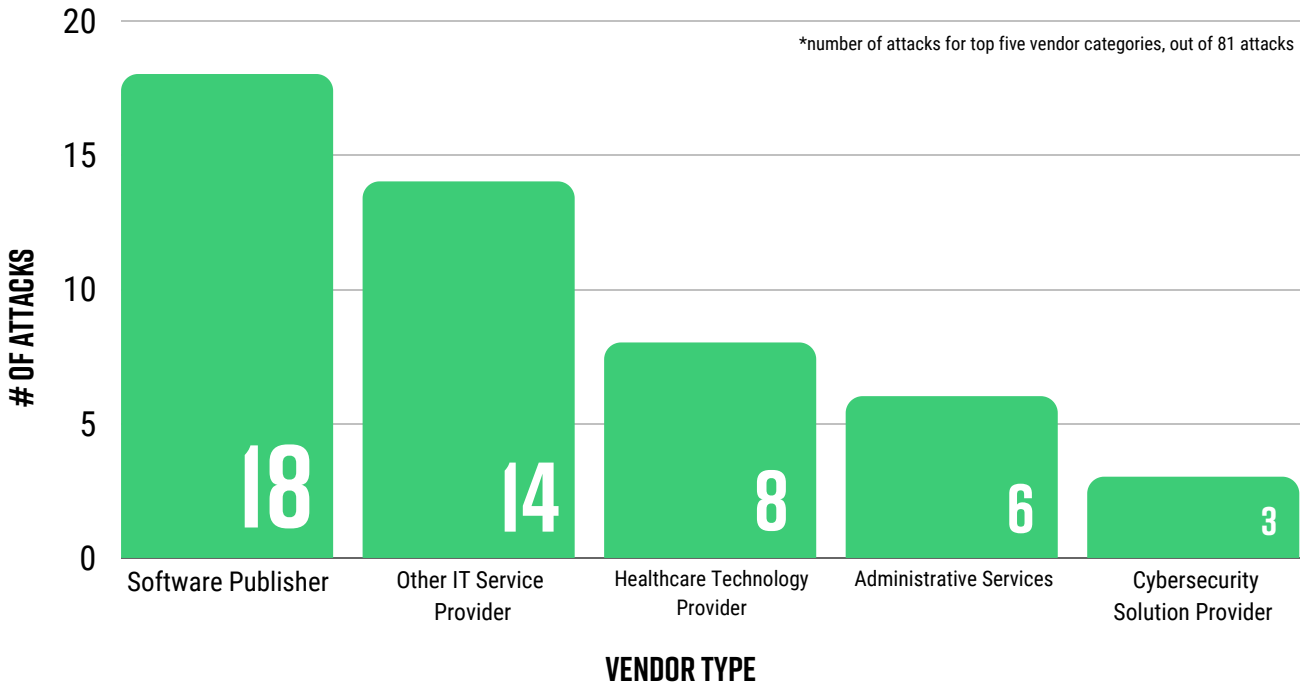
Unsecured servers and databases came in third, accounting for **12% of breaches.** Being among the top three root causes, unsecured external facing assets such as databases and servers pose a major risk to companies. The risk grows much larger when a third party manages PII on behalf of a company or within a shared responsibility agreement. Our studies confirm that the boundaries are blurred when a third party manages that data. In some cases, the companies who are served by the database/server vendor take the idea of security for granted, and do not monitor these vendors until it's too late.

2. GAPS IN VENDOR RISK MANAGEMENT

Software publishers ranked as the most at-risk vendor for third-party breaches for a third consecutive year. A software publisher is a company that develops and markets software, including market research, software production and software distribution. [2]

Hackers find vulnerabilities in software, or edit the code for their own exploitation. Yet, more often than not, companies trust that the software and services they use are secure, and do not check for vulnerabilities along the digital supply chain. Exploitations of weaknesses along the supply chain have led to some of the most notable attacks over the last few years, including 2020's Solar Winds.

TOP BREACHED THIRD-PARTY VENDORS



Having a strong defense strategy means carefully monitoring an entire cyber ecosystem, as opposed to "cherry picking" vendors based on assumed importance. Having merely a checkmark next to a decent rating is not sufficient. A holistic approach to vendor risk management required intelligence from every angle, moving past self-monitoring, and taking the time to see that every last vendor is monitored for vulnerabilities.

3. HIGH REWARD FOR CYBERCRIMINALS

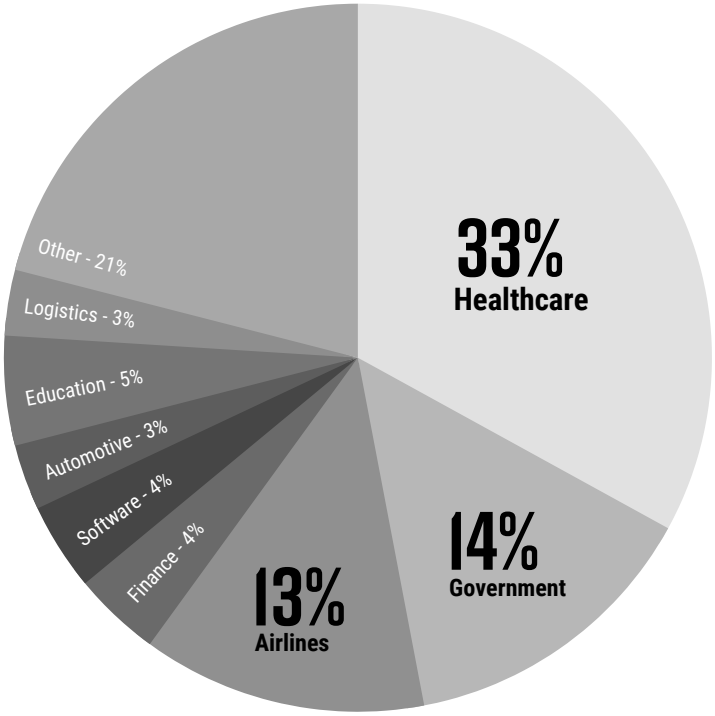
Valuable PII data quickly turns into capital gain, encouraging threat actors to target these opportunistic industries.

INDUSTRIES MOST IMPACTED BY THIRD-PARTY BREACHES

HEALTHCARE

Despite immense cybersecurity improvements following the onset of the Covid-19 global pandemic, the healthcare industry maintained a perpetual target on their back throughout the course of 2021.

In 2021, **1.5 billion users' PII were leaked** as a result of third-party breaches, much of which was healthcare data. A space filled with private patient information and sensitive data, targeting healthcare is a no-brainer for an attacker. Lack of budget, remotely shared personal data between patients and hospital systems, and outdated software all point to avenues for hackers to infiltrate and gain access to a company's data.



GOVERNMENT

Attacks do not discriminate, however the data held by government agencies is valuable, rich and diverse. Consider the vast range of documents and PII data stored; health, social security, and unemployment data are just a handful of the confidential information available to hackers that successfully infiltrate the public sector, not to mention confidential national security information.

Often, databases in the public sector are also out of date and remain unpatched, leaving behind a weak defense strategy and therefore an easy target. Government agencies typically have a wide attack surface as well, from federal down to municipal levels. If a threat actor can achieve access deep within the digital supply chain, it could be months before the effects are truly realized.

4. LACK OF REAL-TIME INSIGHT ACROSS CYBER ECOSYSTEMS

Every second counts when it comes to managing risk, yet many organizations lack the visibility necessary to control threats outside of their own organization.

The average time lapsed between an attack and its disclosure date in 2021 was 75 days. The disclosure date is when involved parties are notified of a breach. This data is based on third party breaches that were transparent about the who, what and when of the attacks. Almost half (44%) of the affected companies are above this average time lapse value.

Unlike advanced persistent threats (APT) that loom over the target network for months, ransomware actors typically aim for fast attacks, and are in a hurry to monetize the incident. Half of the delayed disclosure ransomware attacks included here stem from the Netgain attack in late 2020, where most ripple effects were discovered months later. In unsecured database related attacks, vendors have often assumed a database is protected, leading to late realization of a data leak. Without proper alarms in place, unauthorized network access can also go undetected for months.

The longer the delay, the higher negative impact an organization faces, whether that be millions of dollars or trust from their consumer base. Having a strong incident response plan helps reduce the time between a breach and the disclosure, avoiding further financial and data losses.

The best plans include five important steps: preparation, detection, containment, investigation and recovery. In their annual breach report, IBM [3] revealed that organizations with automated security tactics have an average cost of $2.88 million per breach, compared to a $4.43 million breach cost for those without automated services.

MOST DESTRUCTIVE THIRD-PARTY BREACHES OF 2021

With 81 incidents and 200 publicly disclosed breaches in 2021, several emerged as the most destructive.

1. ACCELLION

The most destructive breach of 2021 was the Accellion FTA breach, impacting 31 companies and over 5.6M users based on the information the vendor and companies disclosed. For scale, that's nearly double the population of Chicago.

On December 23, malicious actors wreaked havoc on users of Accellion's File Transfer Application (FTA). Using a zero-day vulnerability, hackers stole files that were stored on the decades-old server. Although Accellion declared it was patched following discovery, attacks likely occurred throughout late December and early January.

For FTA users, the attack became similar to the SolarWinds breach, where hackers leveraged advanced techniques to gain access into larger organizations through their weaker third parties.

2. CAPTURERX

At a close second was the CaptureRX breach, caused by ransomware. As an administrative service provider to healthcare institutions, the breach affected 121 companies and over 200k users. The majority of leaked data was PHI - protected health information.

3. MEDDATA

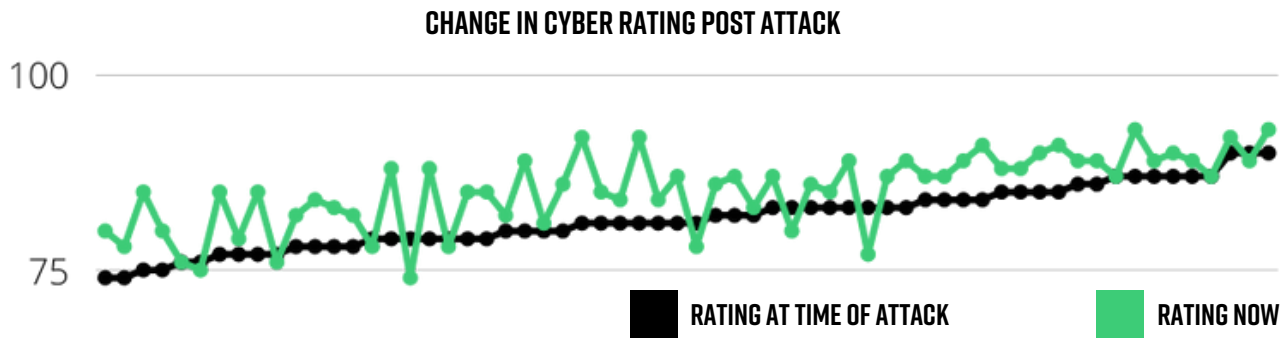
The MedData breach was one of the most high-profile healthcare related breaches of 2021. MedData provides revenue cycle services to healthcare systems and hospitals. In this incident, an employee of a vendor uploaded sensitive patient data on a public Github Arctic Code Vault.

This incident emphasized the need for vendor risk management and strict security policies in healthcare. In light of recent supply chain issues, healthcare organizations should continue to review partnerships with business associates and other vendors to protect against data leaks.

IMPROVEMENTS IN CYBER POSTURE

If we asked if you locked your doors at night, you'd probably say, "Of course I do, why wouldn't I?" If you asked the average Head of Security if they took the same perspective on their cyber risk tactics, you might get a different answer. More often than not, the assumption is that an organization has done enough to get by, until a breach happens.

A cybersecurity researcher is always curious about what happens after a cyberattack. Did the company take enough new measures to prevent this in the future? Did they learn their lesson? Could they have taken more measures preemptively?



On average, a vendor increased its cyber rating by *3.6 points* on Black Kite platform after a breach. **An increase of 3.6 is enough to force a full grade level increase, and could be the difference between a C+ and a B-.** This could easily be the qualifying piece to achieve vendor approval in an onboarding process.

This sample is obtained from a subset of 63 vendors, which were monitored previously. Our research shows that the majority of vendors increased their security posture over time, and only three vendors had considerable decreases in their grades.

As mentioned earlier, the most targeted industries in 2021 were healthcare and government. More than half of the vendors (53%) who increased their grade over time, and over 4 points, were government and healthcare entities. What was their motivation? Preventing another attack.

This increase in posture is astonishing and points to visible change when action steps are put in place. While it is certainly important to improve security posture post-attack, imagine the impact if those steps were taken earlier.

INSIGHT FROM A CISO PERSPECTIVE

from CSO BOB MALEY

What is the agility gap, and how can we close it?

When you look back over time, the numbers and data have shifted. The attack methods may have changed, but what about the bigger picture? What is the evolution of the cyber attacks that we've analyzed?

Threat actors have become more agile over the years, particularly with increased ransomware attacks revealing a sense of heightened agility and skill. This is not just a change from 2021, but an overall message. Attack methods are becoming more clever, more detailed, with flexibility and dexterity. If agile attack methods are improving, our response must match, if not counter their growth.

So what do we do about this? We must address the problem: **the agility gap**.

There are gaps right now in vendor risk management and the way corporate society approaches cyber posture as a whole. If the process remains compliance and checklist-oriented, we forfeit agility for rule following. Checklists create complexity without reaping the rewards of true security. Anyone can check off a box- does it really point to a flexible and mature defense strategy?

A mature vendor risk management program means looking at 200+ places at once in order to slowly close the gaps. Gaps grow larger as soon as you only monitor risk at a single point in time. Real-time insight is the best way to continuously monitor your threat landscape. Cyber criminals are always looking and hunting for the least risky way to reap the highest rewards. Therefore, complicating third party risk management only makes it easier for threat actors to do what they're best at.

If you are going to take one learning away from this, remember that merely following best practices, checklists, and meeting industry standards is outdated methodology for understanding risk. Managing risk with the big picture in mind isn't qualitative, it is flexible. Agility is all about knowing where to look and truly looking isn't process-based.

Use specialized tools to bring up your agility and match the cyber criminals. Most programs are lacking tools with real time insights across cyber ecosystems. If bad actors are experts, we need to become experts too.

ABOUT BLACK KITE

One in four organizations suffered from a cyber attack in the last year, resulting in production, reputation and financial losses. The real problem is adversaries attack companies via third parties, island-hopping their way into target organizations. At Black Kite, we're redefining vendor risk management with the world's first global third-party cyber risk monitoring platform, built from a hacker's perspective.

With 300+ customers across the globe and counting, we're committed to improving the health and safety of the entire planet's cyber ecosystem with the industry's most accurate and comprehensive cyber intelligence. While other security ratings service (SRS) providers try to narrow the scope, Black Kite provides the only standards-based cyber risk assessments that analyze your supply chain's cybersecurity posture from three critical dimensions: technical, financial and compliance.

REFERENCES

[1] **CISOs Connect 2021 Ransomware in Focus**
https://blackkite.com/whitepaper/ransomware-in-focus-new-research-from-a-cisos-perspective/
[2] **PC Mag Encyclopedia**
https://www.pcmag.com/encyclopedia/term/software-publisher
[3] **IBM Cost of a Data Breach Report 2021**
https://www.ibm.com/security/data-breach

CONTACT US

info@blackkite.com

+1 (571) 335-0222

800 Boylston Street, Suite 2905
Boston, MA 02199