2023

BLACK KITE

THIRD PARTY BREACH REPORT

Trends, Shifts, and Lessons Learned from 2022

TABLE OF CONTENTS

INTRODUCTION

This year's report is all about changes. "The only thing that never changes is that everything changes." said Louis L'Amour, the American novelist. Another way of expressing that sentiment is, "change is the only constant."

We are experiencing these changes at an extremely fast pace in the cybersecurity industry. As we all learn from our mistakes, and gain intelligence with experience, so do threat actors. They often learn faster due to lack of boundaries and the luxury to fail. Most enterprises do not have this luxury.

This report, the result of a collective effort of Black Kite Researchers, focuses on what has changed in 2022, for better or for worse, compared to 2021. It highlights some of the lessons of past years and those still being learned within the changing cyber landscape.

In 2022, hackers capitalized on the destructive nature of third party breaches. Although the number of breaches decreased slightly, the magnitude increased significantly, with the number of affected companies per breach nearly doubling. This year, they are certainly targeting killing more birds with one stone.

So what should you do as cybersecurity leaders? You must be as agile as the adversary. The changing landscape forces leaders to add different perspectives to their supply chain risk management. A vendor-specific risk metric is just one example of this perspective.

This report is a compilation and analysis of third party breaches in 2022.

Black Kite Research examined emerging attack tactics and the industries that threat actors targeted most in 2022.

The statistics in this report are mainly collected from cybersecurity news outlets, the dark web, telegram channels, and other Black Kite sources, curated multiple times by experts for accuracy and consistency. It should be noted that the actual number of breaches might be larger than the number announced publicly. Thus, the numbers and graphs in this report should be considered a representative set of the disclosed and undisclosed attacks. 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.

For this study, Black Kite Research analyzed 63 individual third party incidents, which ultimately resulted in more than 298 publicly-disclosed headline breaches and data leaks during the past year. These events inevitably caused thousands of other ripple-effect breaches throughout 2022. The report finalizes the lessons learned and relevant recommendations for the future.

KEY FINDINGS

- In 2022, **63 attacks on vendors caused third party breaches:** from those 63 attacks, **298 data breaches occurred** across impacted companies. In conclusion: 63 hits and at least 298 victims.

- The **level of breach impact and destruction almost doubled** in 2022, with **4.73 affected companies per vendor** (not including said vendor) compared to 2.46 companies per vendor in 2021.
- **Unauthorized network access** emerged as the most common root cause of third-party attacks, initiating **40% of the third party breaches** analyzed. *The method of unauthorized network access is usually not disclosed or discovered. It is often through open critical ports (SMB or RDP ports) or through the exploitation of critical vulnerabilities that lead to unauthenticated remote-code execution.*
- **Threat actors that made headlines by name were primarily ransomware actors** (though many remained anonymous).
- **Ransomware accounted for 27%** of third party breaches in 2022.
- Technical service vendors (those providing infrastructure services) were the top target of third party breaches. These vendors were targeted in 30% of incidents.

- The **healthcare industry**, consistent with last year, was **the most common victim** in third party breaches, accounting for **34.9% of incidents** in 2022.
- 27% of the analyzed attacks began in 2021; the connected breaches and disclosures lapsed into 2022.
- The average time between an attack and the disclosure date was 108 days, an increase from 2021 by 50%.
- Nearly half (**44%) of attacked vendors improved their cyber rating** after the incident.
- Vendors that improved their cyber rating by more than 4 points in 2022 were mostly healthcare vendors (60%), followed by financial services vendors (25%).

EVOLUTION OF THIRD PARTY BREACHES IN 2022

ATTACK DISCLOSURE.

In 2022, 27% of the data leaks announced by companies were due to attacks that occurred in 2021. This begs us to question the evolution of the disclosure time for third party attacks this year.

The **average disclosure time** (time between an attack and the date it was disclosed) **in 2022 was 108 days,** with one attack spanning 408 days. This metric has worsened in 2022 compared to 2021, when the average disclosure time was only 75 days. With an entire month of time added, threat actors have an increased potential for damage with the stolen data.

According to a 2022 report by the Ponemon Institute [1]: *Data Risk in the Third-Party Ecosystem,* **only 34% of organizations are confident their suppliers or primary third parties would notify them of a breach of their sensitive information**. Coupled with the dramatic increase in disclosure time, it has never been more crucial to stay aware of vulnerabilities within all third parties in a digital ecosystem.

ATTACK FREQUENCY.

Although the number of third-party breaches decreased compared to last year, the **individual effect of each breach nearly doubled.**

While the average number of **companies affected by a single breach** was 2.46 in 2021 (not counting the vendor itself), in 2022, this number **increased to 4.73**. These numbers represent publicly announced companies. (There are also bulk numbers for which the name of the companies are not disclosed - meaning the final numbers are much higher.)

2.46

Companies affected by a single breach.

2021

4.73

Companies affected by a single breach.

2022

One could easily speculate that hackers are conducting smarter attacks, aiming for more initiatives that garner a higher number of victims from a single strike. It is of no surprise that over time, the threat actor community has learned to make the most of each attack, hence pivoting to more profitable business models. Ransomware, in particular **RaaS** (ransomware as a service,) are business models that have ramped up over the last few years.

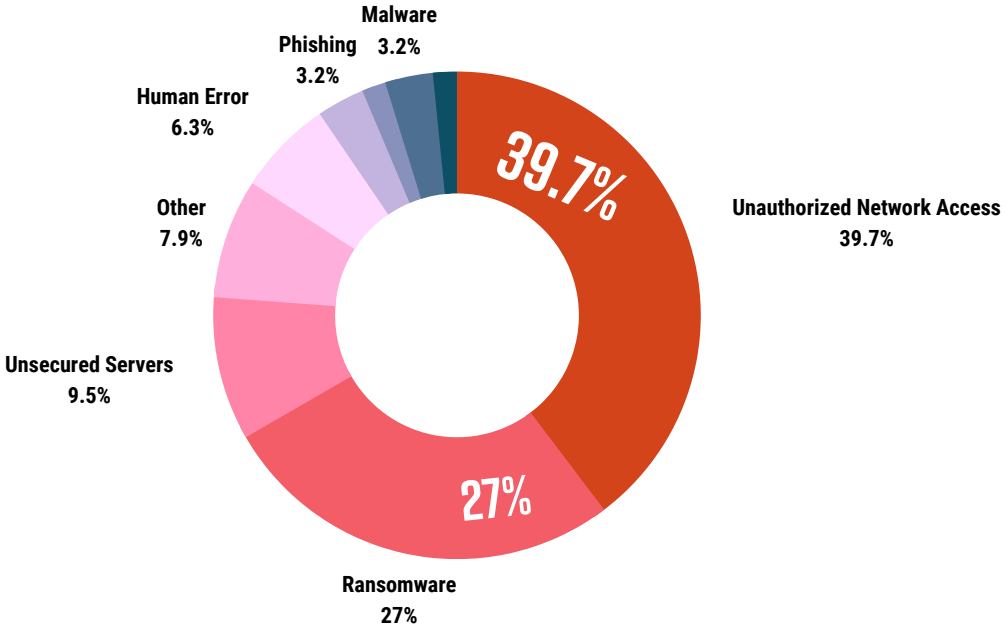
With the **impact of third party breaches doubling this year,** understanding even a vendor's basic cyber posture is an important part of the equation.

THIS IS CASCADING RISK.

*Cascading risk is the **chain of causality that emerges when risk and accumulated vulnerabilities connect** to increase the chance of attack. In simpler terms, cascading risk is the domino effect that occurs when one vendor in a digital supply chain cascades risk and exposure to the rest of their connected vendors (including your organization) in the case of a cyber incident.*

what were the main attack methods?

ROOT CAUSES OF THIRD PARTY BREACHES IN 2022



The initiating vector of a data breach is always important in understanding the behind-the-scenes of an attack. While some companies disclose every little detail as to the "how, what, when" of an attack, some keep the details to themselves.

UNAUTHORIZED NETWORK ACCESS

Unauthorized network access was the most-common attack vector in 2022, accounting for 40% of the third party breaches over the year, with a 25% increase from 2021.

Unauthorized network access is often more complex than it sounds and usually comes with social engineering attacks, primarily phishing. The unauthorized parties access network credentials through phishing, stolen credentials, vulnerabilities in access control, or a combination of these.

Unfortunately, the remote work model that has become prevalent with the pandemic is one of the key enablers for such attacks. Companies should stick to periodic cyber security training for such attacks in the IT department and their employees in other departments.

RANSOMWARE (AND IT'S DECREASE IN FREQUENCY)

Ransomware was the second most frequent root cause in 2022, accounting for 27% of third party breaches, but indicating a decrease from 2021.

One possible reason for this decrease is that threat actors paused ransomware attacks due to the Russia-Ukraine war. Along with this, a number of sanctions were announced against Russia, including banking restrictions. These restrictions are believed to hinder the ability of Russian-based cybercriminals to buy or rent internet infrastructure and cash out the proceeds from ransomware scams.

We can see that many ransomware groups disbanded or continue as smaller groups due to these and other factors. This is a good example of threat actors being forced to change tactics and target less companies with ransomware (for now).

WHAT DO WE KNOW ABOUT THREAT ACTORS?

We know less about the threat actors behind the attacks than last year. Other than threat actors Conti, CLop, Hive, and Lapsus, there is a lack of clear information regarding the remainder. The revealed threat actors are ransomware groups, often seeking recognition and clout rather than staying under the radar.

UNSECURED SERVERS AND DATABASES

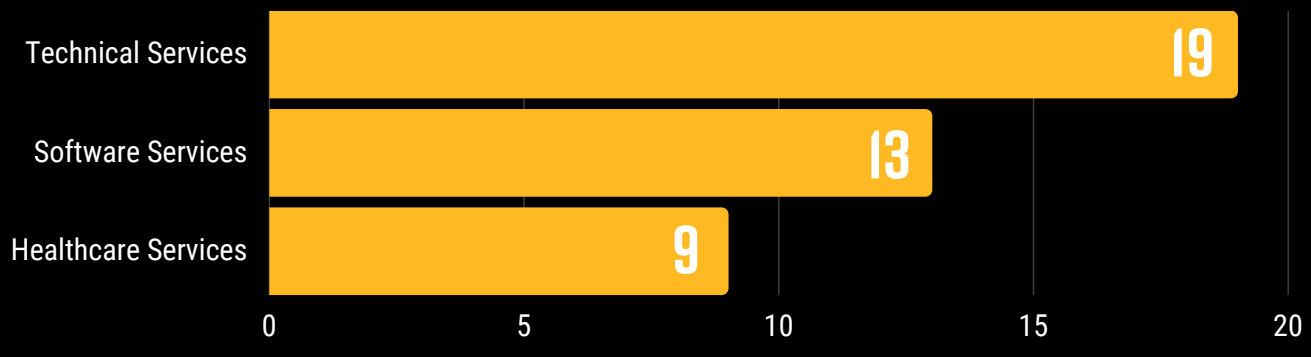
Unsecured servers and databases were ranked third in 2022, accounting for 10% of the breaches. Unsecured assets such as databases and servers pose a great risk to companies and allow for easy entry for threat actors. The risk is even greater when a third party manages PII on behalf of a company, or under a joint liability agreement.

MISCONFIGURED SERVERS

Although we do not include misconfigured server-caused incidents as third party breaches (excluding a vendor's leak due to a misconfigured server), the companies often feel confused on who is to blame for this kind of occurrence. It is common for companies to blame their cloud vendor for leaking sensitive data, being unaware of the "shared responsibility" model. In the IaaS (infrastructure as a service) delivery model, a vendor provides a wide range of computing resources such as virtualized servers, storage, and network equipment over the internet. However, the company itself is responsible for maintaining the security of any information they own or install on the cloud infrastructure.

Server misconfiguration attacks exploit configuration weaknesses found in web servers and application servers. This often leads to security vulnerabilities. The biggest reason these attacks cause breaches is that those cloud companies or advertising companies assume that the security aspect is in the hands of the company they have serviced. There is no direct attack on the company itself here. Leaks occur due to the cloud companies leaving data unprotected.

THE MOST FREQUENTLY BREACHED THIRD PARTIES



Technology vendors were the most at-risk vendor for third-party breaches. Hackers can find vulnerabilities in software or edit the code for their exploitation. Yet, more often than not, companies trust that the software and services they use are secure, failing to 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.

WHAT INDUSTRIES WERE MOST IMPACTED BY THESE ATTACKS?

01. Healthcare

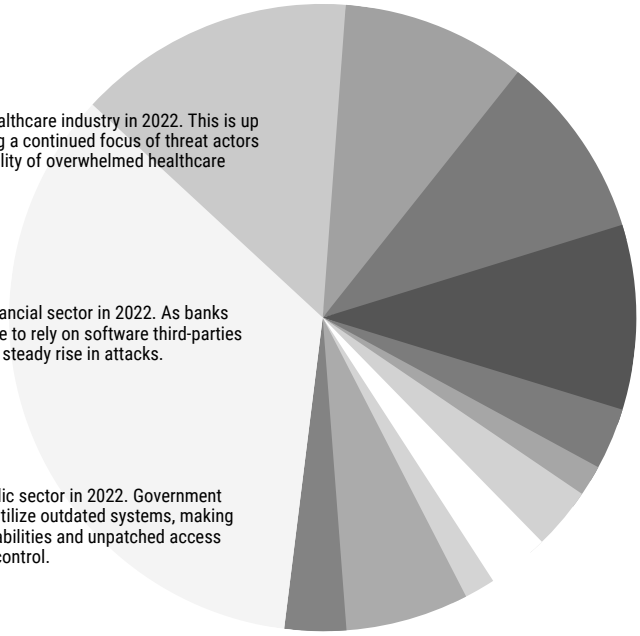
34.9% of attacks targeted the healthcare industry in 2022. This is up one percent from 2021, indicating a continued focus of threat actors on the sensitive PII and vulnerability of overwhelmed healthcare systems across the globe.

02. Finance

14.3% of attacks targeted the financial sector in 2022. As banks and financial institutions continue to rely on software third-parties to provide services, we will see a steady rise in attacks.

03. Government

9.5% of attacks targeted the public sector in 2022. Government organizations and groups often utilize outdated systems, making them more susceptible to vulnerabilities and unpatched access points for threat actors to seize control.



HEALTHCARE

In 2021, 33% of the attacks that caused breaches were in the healthcare sector. This year the percentage increased slightly, coming in at **34.9%**. One of the main events that caught hackers' attention to healthcare was Covid-19. While everyone in the world concentrated on the health sector, tremendous data began to pile up within the healthcare realm.

Regulations like HIPAA and GDPR are very strict on how to handle the data, due to the high risk. However, the heavy sanctions for breaches of personal health information (PHI) have only attracted more attention to this sector. 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 health-related sensitive data. That's why, again this year, the most affected sector has been healthcare.

This year, a **ransomware** attack was carried out on Colorado-based, **Professional Finance Company**, known as PFC, a debt collection firm which serves hundreds of companies in the health sector in the United States. It was the second largest data leak this year after Shields Health Care Group's data breach in March, affecting 2 million patients.

PFC, which had contracted thousands of organizations to process unpaid invoices and unpaid balances of customers and patients, announced on July 1 that it had been hit by ransomware in February. In its data breach notification, *PFC noted that more than 650 healthcare providers were affected by the ransomware attack.* They shared that the attackers obtained patients' names, addresses, outstanding balances, and information about their accounts.

PFC said that in some instances, birthdates, Social Security numbers, health insurance and medical treatment information were also obtained by the threat actors. Later on, in a separate filing with the U.S. Department of Health and Human Services, PFC announced that more than 1.91 million patients were and are affected by the ransomware attack.

The healthcare industry is particularly interesting when it comes to third party attacks due to the HIPAA Breach Notification Rule and the HIPAA Privacy Rule. These govern federal disclosure requirements for alleged breaches upon the majority of healthcare organizations [2].

Under HIPPA, third party organizations must notify any associated healthcare organization within 60 days discovering a data breach. From there, the healthcare organizations must notify affected patients or individuals within the data compromise. In an attempt to avoid these cyber events, the HIPPA Security Rule requires healthcare entities to complete regular risk assessments on the security systems set in place.

FINANCE

The second sector most affected by third party attacks in 2022 was the financial sector. Banks and financial institutions are typically the most vulnerable businesses to data breaches. Often third party fintech service providers are targeted, on which banks and financial institutions rely significantly.

Banks work with many vendors for faster transactions and applications, such as credit management. As a result, they grant access to sensitive data, vital systems, and other critical resources. Unfortunately, these financial service providers do not adequately take reasonable precautions to keep this data safe.

GOVERNMENT

Public sector organizations continued to be highly targeted by third party attacks. The data held by government agencies is valuable and diverse, often pertaining to critical infrastructure. Their systems house all citizens' personal information, including health data, Social Security information, unemployment data, and confidential national security information.

Organizations within the public sector with such valuable and diverse data cannot escape the attention of threat actors. Unfortunately, public sector databases lack adequate security measures, leaving behind a weak defense strategy and, thus, an easy target. Moreover, government agencies are present in almost every sector, and they have many vendors, creating a vast digital supply chain.

THOUGHTS FROM A CISO: WITH BOB MALEY

In the August 2022 IEEE article "Closing the Agility Gap," we discussed the evolution of cyber-criminal behavior and their continued improvements in skills and agility [3].

The findings in this report give further credence to that gap; following best practices in third party risk management is just not keeping up with the bad actors. It is still all about basic blocking and tackling, the quick fixes, and changing how we view third parties to how bad actors see them.

who did the attacking?

TOP 5 THIRD PARTY BREACHES OF 2022

1. TOYOTA

One of the most notorious breaches this year hit Japanese automaker Toyota. Toyota announced in October that it had mistakenly disclosed a credential, allowing access to customer data in a public GitHub repository for nearly five years. Toyota suffered a massive data breach after the T-Connect application released its source code on Github, a software development platform, in December 2017. Unfortunately too late, Toyota did change the access code after realizing this, on September 15, 2022. Of course, Toyota could not prevent the exposure of 300,000 customer emails.

This is not the only event Toyota experienced in 2022. Toyota suffered a cyberattack on February 28, resulting in a 3-day suspension of production at its factories. After this attack, Kojima Industries, which manufactures both interior and exterior auto parts and is part of Toyota's supply chain in Japan, was also affected. This attack resulted in the suspension of production at 14 factories and 28 production lines.

2. ILLUMINATE EDUCATION

Education technology vendor, Illuminate Education, reported a major data breach in early 2022 that affected millions of current and former NYC students within its system. Parents trusted Illuminate Education with their children's personal information, and assumed the company would take their privacy concerns seriously. Unfortunately, this did not happen, and due to the data breach, students' names, birthdays, ethnicities, languages spoken, and student ID numbers dating back to the 2016-2017 academic year were compromised.

In addition, the breach endangered students and special education services, classrooms, and teacher programs to unauthorized parties. It even allowed them access to information about whether or not they received a free lunch. While we don't know why hackers are targeting organizations like Illuminate Education, we do know that threat actors love companies with weak data security systems and vulnerabilities in their networks. Illuminate Education was the first company to be kicked out of the Student Privacy Pledge because of this data breach and misrepresentation of its security measures.

THOUGHTS FROM THE HEAD OF RESEARCH: WITH FERHAT DIKBIYIK

This year, threat actors, especially ransomware groups, targeted less third parties, but reached more victims compared to the previous year.

Apparently, this "less is more" strategy has worked for them, considering the data breaches experienced in 2022.

Adversaries select the most impactful vendors in the ecosystem to increase the attack surface. The most impactful vendors create the concentration risk in the larger vendor ecosystem, and IT/Software vendors are at the top of the lists of threat actors. Among other risk indicators, concentration risk should be another critical metric for third-party cyber risk experts.

who did the attacking?

TOP 5 THIRD PARTY BREACHES OF 2022

3. HIGHMARK HEALTH

In March 2022, Highmark Health in the United States confirmed a data breach resulting from an incident involving their computer network. The information of 67,147 individuals with mailings about prescription drug changes was exposed, including their names, dates of birth, Highmark member IDs, and prescription information. In recent years, companies in the health sector have begun to store information electronically to facilitate the protection of consumer data in their businesses and organizations. But electronic storage exposes information to the risk of being compromised. Recent studies have shown that 15 million people have been victims of identity theft. Many identity theft cases occur due to data breaches, such as the case announced by Highmark Health.

4. MAILCHIMP

In April 2022, Mailchimp, the third-party newsletter provider used for marketing communications, was discovered to be compromised repeatedly for several months. Four Mailchimp employees were targeted by phishing campaigns for weeks, resulting in them providing secure access keys to the attackers. Hackers were able to view approximately 300 Mailchimp accounts and successfully export audience data from 102 of those.

On August 8, Digital Ocean (a company using Mailchimp) announced that its engineering team noticed that MailChimp had stopped delivering emails such as confirmations, password resets, email-based alerts for product health, and dozens of other transactional emails. The reason for this outage was that Mailchimp suspended the Digital Ocean account without any warning or explanation following the attack.

DID YOU KNOW?

Black Kite tracks high-profile events in our platform using FocusTags™, keeping all customers aware of any additional vulnerabilities they may be experiencing risk from.

5. OPENSEA

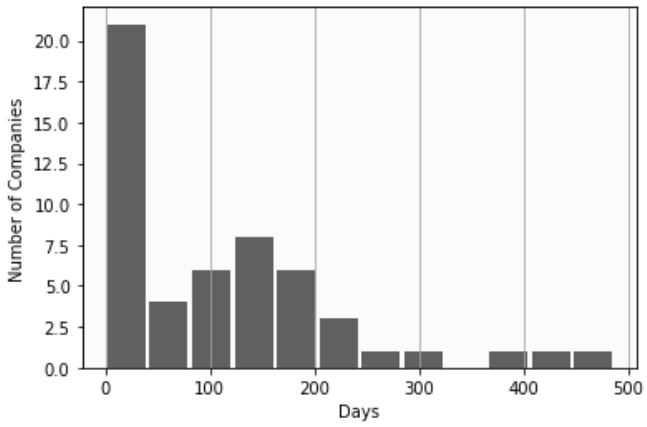
On June 29, OpenSea announced that an employee of Customer.io, their email delivery vendor, had misused their employee access to download and share email addresses – provided by OpenSea users and subscribers to their newsletter – with an unauthorized external party. According to the blog post, the leaked information included email addresses, and OpenSea warned users that this could result in “a heightened likelihood for email phishing attempts.”

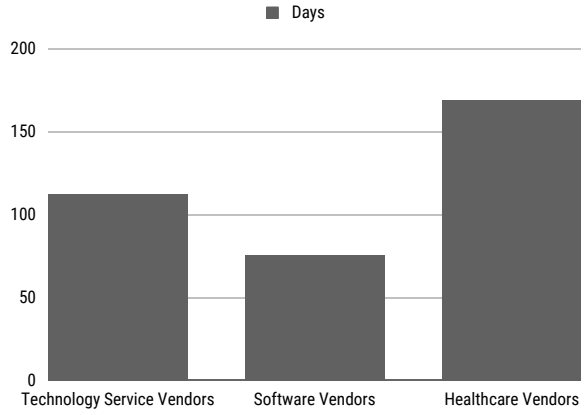
The company announced that customers should assume they have been impacted by the news if they had shared their email address with OpenSea in the past. The breach was not caused by OpenSea itself, the firm explained. Rather, it was due to an employee of Customer.io, a third-party platform hired by OpenSea to manage social media communications.

Hubspot, a platform similar to Customer.io, was hacked in March, affecting BlockFi, Swan Bitcoin, NYDIG, and Circle. Additionally last month, OpenSea discovered its Discord server was compromised and flooded with phishing advertisements promoting a scam NFT.

THE AFTERMATH OF AN ATTACK

As mentioned earlier, breach reporting times are often still too slow and appear to be getting worse. The average breach disclosure time in 2022 was 108 days, 50% more time than in 2021. *Black Kite has been tracking this statistic since 2021.*





This data is based on third party incidents that were followed up with transparency about the who, what, and when of the attacks. Black Kite started monitoring this statistic in 2021, and the immediate conclusion is that it is getting worse. Why? Let's first take a look at the regulations.

With all the regulations like HIPAA, spoken about above, and GDPR, organizations are required to report certain types of personal data breaches to the relevant supervisory authority. More specifically, Article 33 of GDPR says that, in the event of a personal data breach, data controllers should notify the appropriate supervisory authority without undue delay and, where feasible, no later than 72 hours after becoming aware of it. The NYDFS cybersecurity regulations also require a 72-hour notification during a cybersecurity event, and California's CCPA has a similar requirement.

HIPAA's rule, on the other hand, dictates that *"If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches annually. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered." [4]*

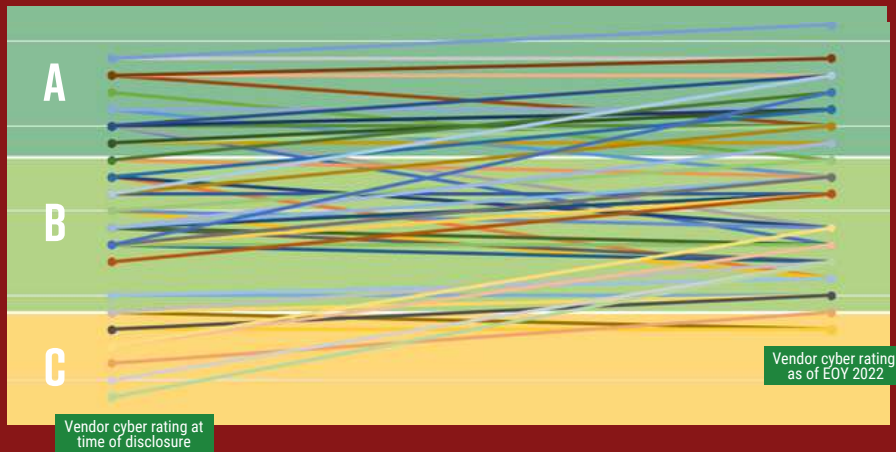
Software vendors have the least disclosure days, with an average of **75 days,** followed by technology service vendors with an average of **112 days.** Healthcare has the highest disclosure time period, at **169 days on average.**

YOU'VE BEEN ATTACKED. WHAT NOW?

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 the measures preemptively?

When we look at the post-attack phase, we see that the vendors that have improved their cyber rating within the Black Kite platform by more than 4 points are mostly healthcare vendors (60%). This is followed by financial services vendors at 25%.

50% of vendors increased their rating after the disclosure of an incident. 25% decreased between 1 and 7 points. 23% stayed the same.



LESSONS LEARNED IN 2022

Threat actors (could) ring twice.

While it does not necessarily have to be the same threat actor, your door could be knocked on by a threat actor twice in the same year. This year, five of the companies analyzed were hit twice through different vendors, 3 of them in the information industry.

Names don't make a big difference.

This year, 80% of the attacks that had a threat actor identified were ransomware attacks. Apart from ransomware attacks, almost all incidents remained anonymous.

Pay attention to specific vendors.

If you rely on one single vendor to provide a critical service and that vendor loses the ability to provide it, your operation is severely impacted. Diversify critical processes.

Companies are still lagging in terms of disclosure dates.

Build relationships with your vendors, encouraging a direct line of communication.

Focus on quick fixes.

Credential misuse is still either directly or indirectly used in most attacks.

INSIGHT FROM CYBER EXPERT
JEFFREY WHEATMAN

"No man is an island, entire of itself; every man is a piece of the continent, a part of the main." *John Donne*

I love this quote from 17th century English poet, scholar, soldier and cleric, John Donne. The sentiment is as true today as it was when first said. It is also quite applicable to the problem of third party risk management. Global business ecosystems continue to get more complex, with every organization increasingly impacted by the cybersecurity behavior of their partners, and their partners' partners, on and on.

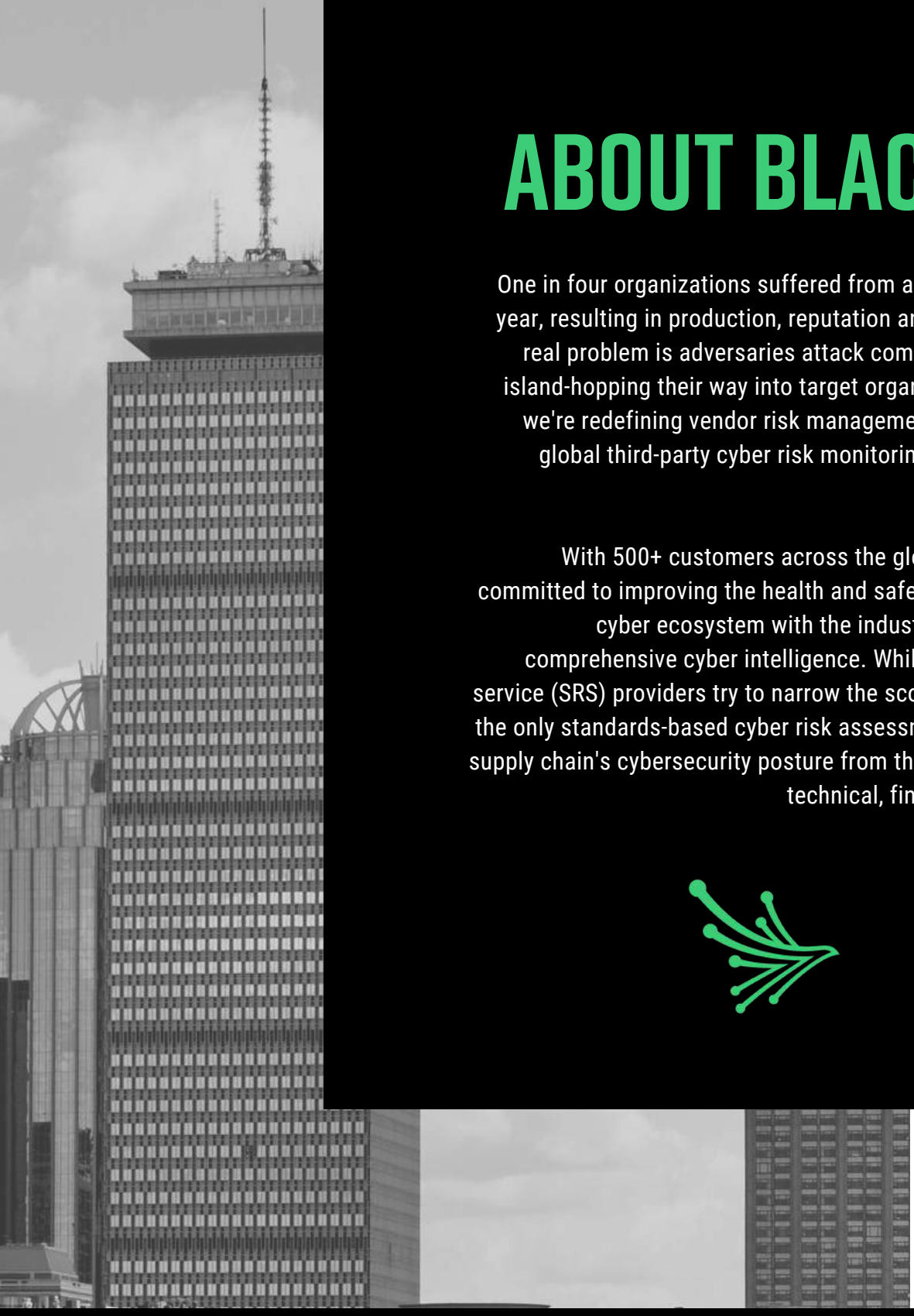
Managing third party risks used to be simple - if legal and finance were satisfied, everyone was happy and contracts were signed. "I's" were dotted, and "t's" were crossed. *No more!* The cyber posture of your partners and supply chain is increasingly impacting your operational goals and objectives.

Imagine if one of your critical suppliers got crushed by the newest ransomware and couldn't function for a week – **how long would you be impacted?** Generally speaking, the answer is much longer than a week. What if a partner was breached and data you collected from your customers gets stolen and released in the wild. Do you think your customers care who actually got pw0ned (they don't)? How many of your critical partners are doing a good job protecting themselves – and by extension protecting you? The reality is most of them are not. **Your attack surface is much bigger than the stuff you control.**

We know Home Depot and Target were breached. We know they were breached via third parties. Does anyone know the name of either of the third parties? Nope! This is one of the many reasons why understanding your operational risks, including those that accrue to you by way of partners, is no longer optional. Supply chain risk is a top board initiative and will be so for the foreseeable future. Understanding the cybersecurity impact on your organization is no longer optional. Point in time questionnaires have never been all that useful; and they have never been accurate. I would bet that plenty of the data in this report belies what organizations wrote up in their questionnaire responses.

The report contains good news and bad news. The good news, **defenders are getting marginally better and the number of breaches via third parties dropped YoY**. The bad news, while the number of breaches dropped, **the impact of the breaches jumped.** And we are seeing a lot of the same issues and vectors for successful attacks - this means *basic blocking and tackling aren't happening.*

While you may not have control over your partner's cybersecurity program, you can assess and monitor your extended ecosystem. After all, **you cannot manage what you cannot (do not) measure (in this case monitor).** **Another one of my favorite quotes from Lord Kelvin.*



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 500+ 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. Data Risk in the Third Party Ecosystem | Ponemon Institute
2. https://www.magmutual.com/learning/article/how-respond-data-breach-third-party/
3. August 2022 IEEE article "Closing the Agility Gap,"
4. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

CONTACT US

info@blackkite.com

+1 (571) 335-0222

800 Boylston Street, Suite 2905
Boston, MA 02199