BLACK KITE

2021 THIRD-PARTY BREACH REPORT

THIRD-PARTY BREACHES ARE ON THE RISE, RESPONSIBLE FOR 69 MAJOR BREACHES IN 2020.

Supply-chain attacks raced through 2020 headlines, including the largest supply-chain attack in the last decade - SolarWinds. Breaches driven by ransomware targeted vulnerable healthcare systems and educational platforms in light of the global pandemic, Covid-19.

In this report, Black Kite researchers examined the 2020 threat landscape to uncover root causes, new-year cybersecurity resolutions and lessons learned.

Methodology

Black Kite analyzed 69 major headline data breaches caused by third parties to uncover the most impacted organizations, the susceptibility of the associated third parties and how each breach was accomplished.

Key Findings

69

major breaches were caused by third parties in 2020

1/4

of breaches stemmed from unsecured cloud assets

23%

of targets in a supply chain were software vendors

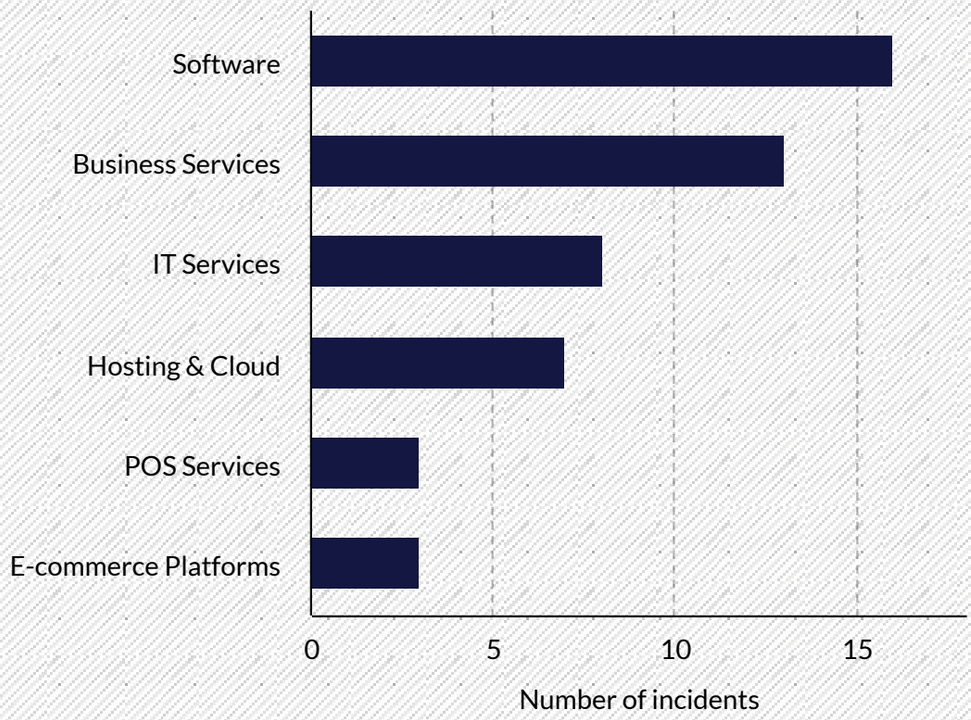
Most Common Targets for Supply Chain Attacks

1 Software Providers

2 Business Services

3 IT Services

Vendors Involved in a Third-Party Breach



#1 Software Vendors

Attacks toward a diverse set of third-party software systems collected personal information and confidential company data. From banking software to employee communications, payment software to channel managers, hackers utilized software vendors as a primary target in 2020.

External software has not been considered as a third party for years for many reasons. First and foremost, the community is used for leveraging external libraries and code pieces. Hundreds of external libraries are utilized on a web page. The pace of software updates, new features and more also makes it difficult to devise continuous auditing, leaving the systems as the weakest links in a supply chain.

- American Bank Systems (ABS), a U.S. bank service provider, was targeted through a ransomware attack, resulting in **53 GB**

Resolution #1

Act quickly. The consequences of a breach can be dire. Slow response and disclosure times could result in additional lawsuits.

of data leaked from financial institutions. The loan documents confiscated included customer names, tax ID numbers, business contracts, personal email addresses, invoices, credentials for network shares, company confidential files, and other personal information.

ABS was handed a class-action lawsuit due to its failure to protect customer information, as well as not notifying customers in a timely manner after the initial ransomware attack.

Prestige Software, a channel manager linking hotel reservations to sites like Hotels.com, Booking.com, and Expedia, revealed millions of hotel guest records following a data breach. The company's hospitality cloud software was storing guest data on an unsecured Amazon Web Services cloud database for seven years, which leaked financial data as well as reservation details.

Insurance tech company **Vertafore's** negligence **compromised data for 27.7 million drivers** in Texas. The company blamed the incident on human error, after discovering the drivers licenses were accessible through the company's unsecured storage.

#2 Business Services

Business services include a variety of resources, such as insurance and benefits, accounting services, and more— many of which were leveraged by hackers to gain access to larger accounts. In 2020, this included:

ViewMedia, a marketing vendor serving major American publishing brands including Tribune Media and Times Media Group left an Amazon S3 bucket unsecured. Along with personal data, the bucket included thousands of marketing newsletters, promotional flyer designs, banner advertising, and declaration of work documents produced for its customers.

Resolution #2

Adopt a data-centric attitude in vendor classification. Know where your data resides.

A leak in **Canon's** business process services eventually compromised General Electric's past and present employees. A wealth of employee data was among the leak, including Social Security numbers, driver's license numbers, bank account numbers, and passport numbers.

Chubb, a global cybersecurity insurance and training services provider, was a target of a ransomware attack by the Maze group. Given that Chubb is one of the largest cybersecurity companies in the U.S. and provides training to other companies, the attack has garnered attention nationwide.

#3 IT Services

SolarWinds was the protagonist of the largest supply-chain hack in the last decade. Beginning with FireEye, the extent of the attack spread to government organizations such as the U.S. Departments of Defense, State, Treasury, Homeland Security and Commerce, and more.

The United States Administrative Office (AO) is now investigating whether court reports in succeeding trials have also been accessed by hackers. It's unknown if and what details have been secured that could still affect U.S. government agencies in the coming months.

Cognizant was another victim. Targeted by the Maze ransomware attack, several internal systems were disabled, forcing other systems to be taken offline. As a result, Cognizant expects to pay further legal and consulting fees, and to incur costs for restoring services and remediating the security breach.

Resolution #3

Strengthen crisis management to ensure business continuity.
Preparation is key.

DISCOVER THE SOLARWINDS ATTACK FROM A HACKER'S PERSPECTIVE

#4 Hosting & Cloud Services

Many companies use cloud services to store sensitive data and execute cloud-based applications. Companies also leverage hosting providers to manage their websites. Although cloud and hosting providers are usually secure, sometimes the misconfiguration of servers or cyber attacks expose sensitive data in these environments.

Blackbaud, a cloud and CRM company specializing in non-profit organizations, was by far the most devastating supply-chain attack on healthcare in 2020. The hack quickly evolved into a global set of incidents, creating a ripple-effect beginning in May of 2020. The aftermath was disclosed in July, **two months after the initial discovery**.

Hackers also attacked **a web-hosting firm** that provided services to over 200 law enforcement and government agencies throughout the United States, **exposing nearly 270 gigabytes of potentially sensitive data** from fusion centers and police departments nationwide.

Resolution #4

Keep tabs on all your services, even if they typically pose a lower threat. The ripple-effect could be catastrophic.

#5 E-commerce Platforms

Around 2000 e-commerce stores running the **Magento** program were targeted on August 2020, compromising thousands of customer's information.

The stores were running an older version of the Adobe™ Magento software, in which Adobe ended the support in June. Magento is an open-source e-commerce platform written in PHP code, which was acquired by Adobe in 2018.

According to our research, about **38,000 e-commerce sites still rely on the older version** and could be affected.

Resolution #5

Patch older systems and versions. More than 50% of common security vulnerabilities exploited by cybercriminals are more than one year old.

Resolution #6

Leverage cyber intelligence sources. *Dark Web Monitoring* should be utilized for both pre-breaches and post-breaches.

#6 POS Services

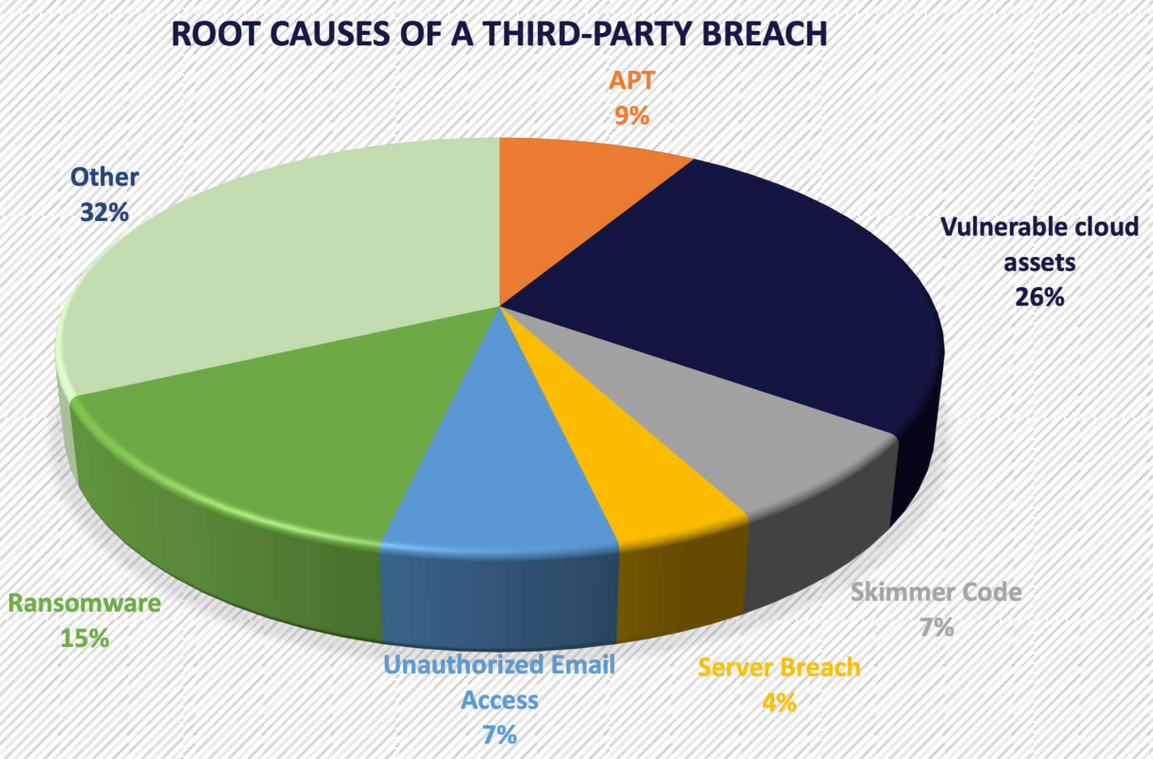
Rutters, a U.S.-based convenience store chain, disclosed a security breach affecting its customers shopping via POS devices in Pennsylvania and West Virginia stores. The malware targeted the POS devices, collecting customers' payment details within convenience stores and several of the company's fuel pumps.

Our research revealed **1/3 of locations across 30 states** were affected. The breach went unnoticed for over a year until it was discovered to be publicly available on Joker's Stash.

As a result, franchises like Dickey's Barbecue Pit could have as many as **3 million cards for sale** on the dark web.

ROOT CAUSES OF A BREACH

Following these third party attacks, we explored root causes to better understand the initial points of intrusion. **Vulnerable cloud assets, ransomware and APTs** surfaced as the top three sources.



Vulnerable Cloud Assets

1/4

of third-party breaches stemmed from vulnerable cloud assets.

Many companies use cloud servers to store their data. Despite their great advantage, misconfigured databases including AWS buckets expose sensitive data, serving as an open invitation to hackers to use a company's data for malicious activities.

Ransomware

#1

source of a breach on insurance claims

With the pandemic, remote workforces have created new and enticing vectors for cybercriminals to execute ransomware. The Blackbaud breach, due to ransomware, created a ripple effect for the healthcare industry. For a detailed case-study on ransomware on third parties, click here.

APT

10%

signalled for an APT presence

An APT establishes a long-term presence on a network to mine sensitive data. APT groups and their attacks towards supply-chain began to spike in 2020 as an effective breeding ground. These groups place a malicious backdoor on a vendor and expand the threat landscape through software updates or toolkit downloads.

THIRD PARTIES REQUIRE THE SAME DUE DILIGENCE AS ORGANIZATIONAL PROTECTION

LESSONS LEARNED FROM 2020 BREACHES

Supply Chain Security

Third party risk monitoring is no longer a nice-to-have, it's imperative. Hackers prey on vendors or third parties instead of main targets because they serve as a more vulnerable outlet. No matter the strength of your internal security, vulnerable third-party products can serve as a loophole. Companies should leverage an automated tool to continuously monitor the security posture of their vendors.

Boards

Boards are liable for cybersecurity breaches, no matter the origin. It's important that boards obtain a deeper understanding of cybersecurity. CISOs should also take the leadership in board-level cybersecurity decisions.

Breach Disclosure

Companies incur various costs due to breaches. Financial penalties and legal costs account for a large portion of these penalties. Disclosing breaches at an early stage helps vendors in your ecosystem contain the breach quickly and prevents further penalties. GDPR requires notifications be made within a 72-hour window upon discovery of a qualifying breach.

Adopt a Data-Centric Mindset

Know where your data resides in the entire ecosystem. Organizations often experience unprecedented data challenges, resulting in data leaked to vendor Amazon buckets or portals your organization leverages for business activities.

DevSecOps

Integrating security into the DevOps cycle and adopting a holistic DevSecOps process is imperative, especially with the exponential growth of open-source software. From private keys to access rights, securing your operations at every point that each line of code traverses is critical to the process. Using automation will make this process scalable.

Patch, Patch, Patch

More than 50% of common security vulnerabilities exploited by criminals to execute cyberattacks are more than a year old. IT teams become overwhelmed and miss critical updates under the mounds of bugs, CVE codes, severities, patches, and workarounds. A security automation tool with risk prioritization will always help the teams stay up-to-date with critical alerts.

BLACK KITE'S TAKE

We know there is no magic bullet in cybersecurity. An effective program starts by understanding the landscape, which includes third party ecosystems and incident response capabilities. This knowledge will help organizations quickly identify and reduce their potential risk.

This requires much deeper level of analysis and more agile response. Integrating the right risk mitigation tools that account for real-world potential impact is now a must in 2021.

Without that view, insights simply become friction.

VISIT OUR WEBSITE

for more information on data breaches caused by third parties

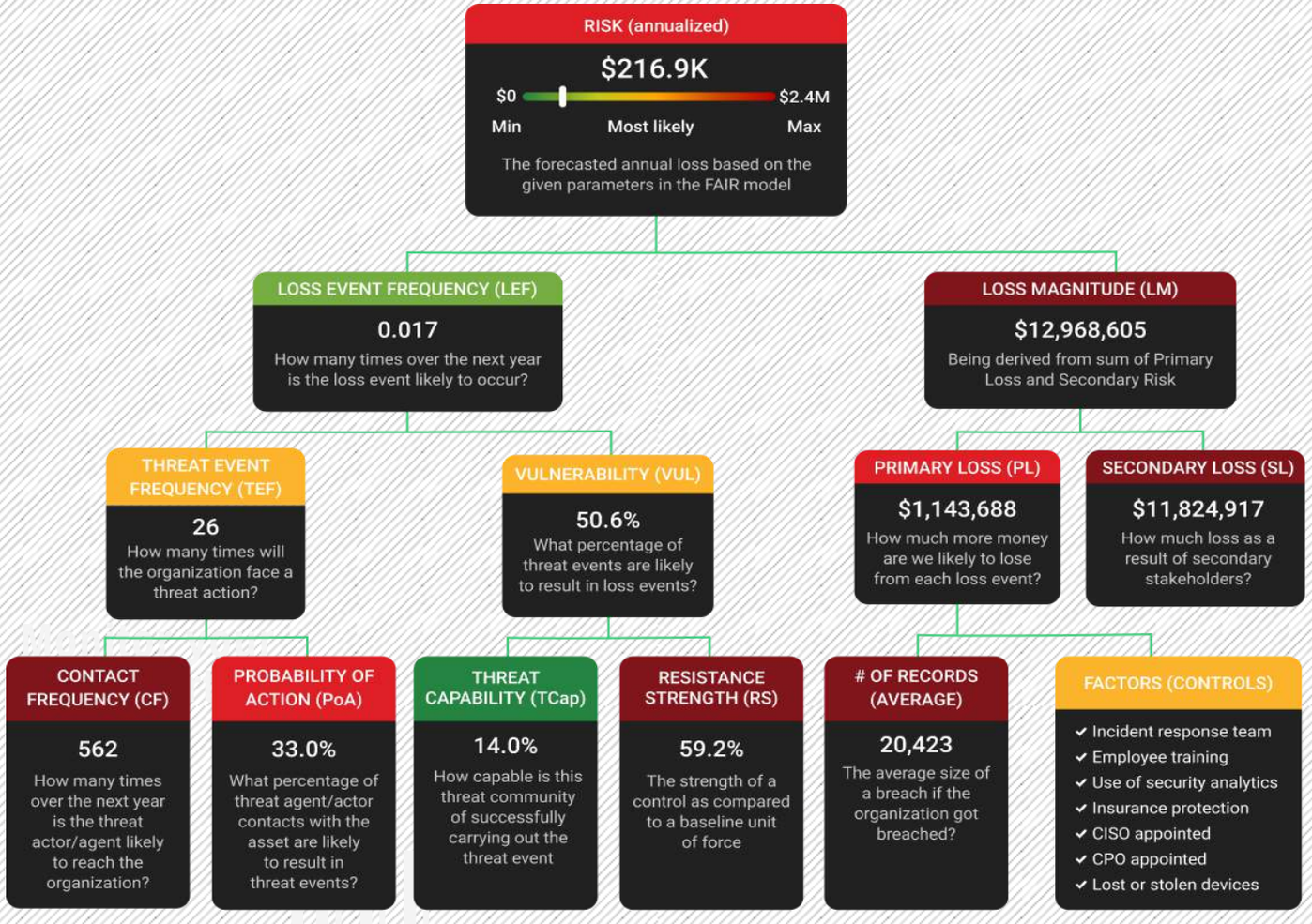
CLEAR THE NOISE.

Mature Your Third-Party Risk Management Program with Risk Quantification

For cyber risk professionals looking to quantify and maintain visibility of their risk exposure, Black Kite provides a defensible platform that spans the entirety of the third-party risk management life cycle.

Our rating technology uses open-source intelligence to compare vendor cybersecurity to industry standards. Black Kite is also the only cyber rating system that puts a dollar value on risk, using OpenFAIR to quantify risk in financial terms.

By eliminating false positives and providing tools to fix risk levels across their externally facing digital footprint, our platform makes organizations more resilient.



BLACK KITE

Copyright Black Kite 2021

We regularly monitor and provide updates on third-party data breaches. Discover more on our website.