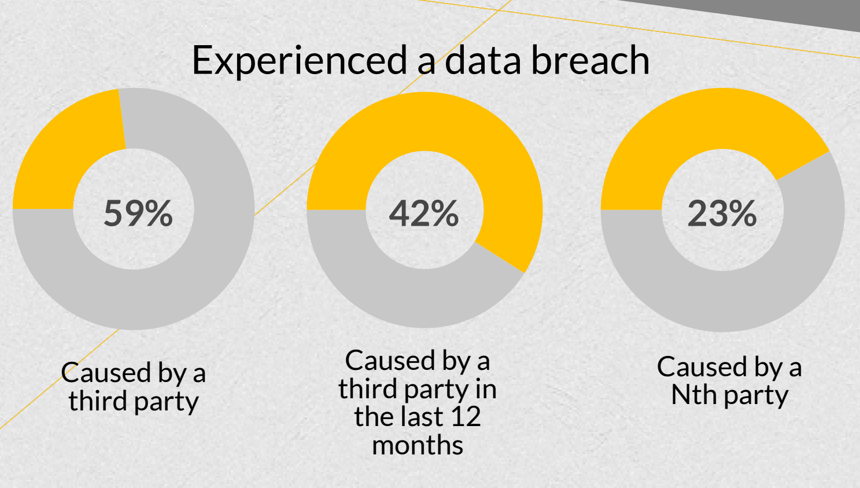
2020 THIRD-PARTY DATA BREACH REPORT

Billions of dollars were spent by corporations and government systems to fend off cyber threats in 2019. Often, their investment isn't enough. Threat actors sneaking through the cracks hit "third parties" to harvest information, leading them to larger organizations. What factors do cyber threat actors use as bait before targeting bigger prey? Black Kite researchers examined 2019's revelations to dig deeper into these loopholes.

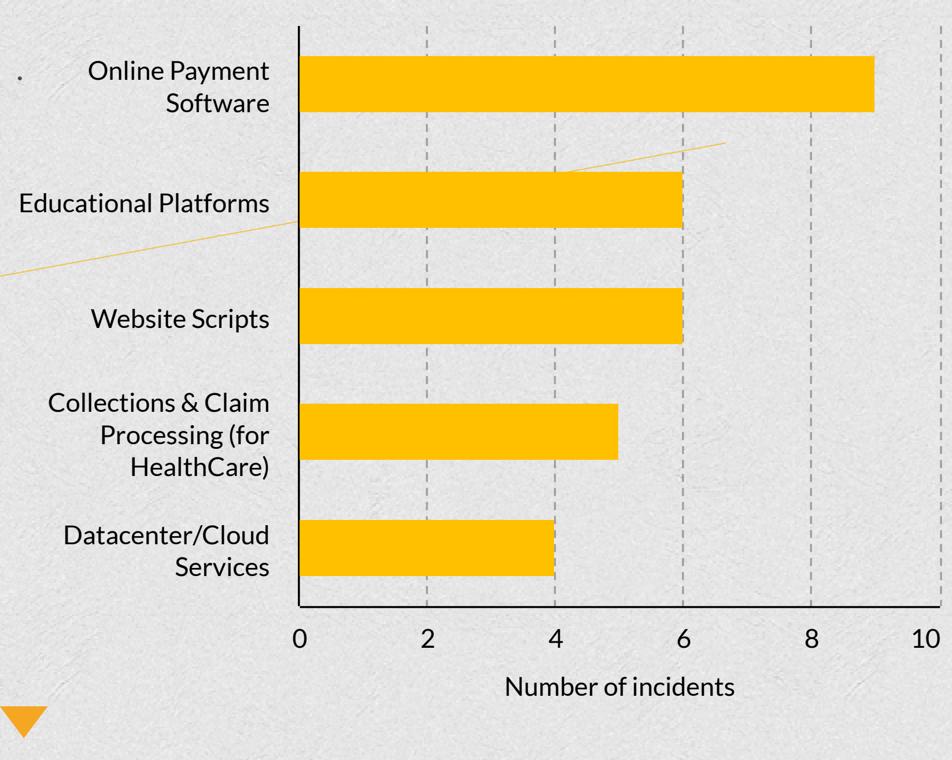
Almost 60% of the companies experienced a data breach caused by a third party

According to the Data Risk in the Third-Party Ecosystem Study from Ponemon Institute


Experienced a data breach

Top 5 uses of a third party

We analyzed 66 major data breaches caused by third parties mentioned in the news in 2019. We asked questions as to whom, what third-party, and how, in search for the culprits behind a breach.



5 Takeaways from 2019 Third-Party Data Breaches

#1 Online payment software: The frontrunner in attracting hackers

In terms of finance-related data breaches, 2019 was a record year. By hacking into the payment software operated by third-parties, hackers gain access to private credit or debit card information.

- Hackers gained access to public credit and debit card information due to a flaw in the Click2Gov utility-payment software. Some of the incidents occurred in utility payment systems of the City of Marietta, City of San Angelo and Pompano Beach City.
- The cities of Saint John in New Brunswick, Canada and Hanover County of Virginia are also recent victims of attacks against Click2Gov's online parking ticket payment. Payment information of 6,000 citizens in Saint John and thousands in Hanover County was compromised.
- A cyber attack targeting PayID, a third-party vendor of an Australia's Westpac Bank, impacted the personal information of almost 100,000 Australians.

Takeaway: Employees are no longer the weakest link. Third parties have quickly assumed this role, including software containing sensitive personal information.

#2 Educational Platform Providers

Learning platforms provide information to support teaching as well as assessing student knowledge. This means these databases hold a wealth of student information, including learning skills that could be harvested by hackers when a platform is breached.

- A breach at Chegg, a popular educational technology company serving George Washington University, affected thousands of the university's community members' information. The breach exposed usernames, passwords, and addresses.
- A data breach on the web platform AIMSweb 1.0, a tool used by educators around the globe, affected tens of educational institutes and some 600,000+ students. The performance assessment tool is used by educators around the globe and operated by Pearson Clinical Assessment.
- The third-party server providing healthcare training services to the Singapore Armed Forces (SAF), was infected with ransomware. The encrypted file on the server contained personal data of 98,000 SAF servicemen possibly exposed full names and NRIC numbers of the staff.

Takeaway: Consider the sensitivity level of personal information that resides in your organization and beyond your perimeter. Keep track of where your data extends.

#3 Website Scripts: The Malicious Ones

The famous British Airways and Ticket Master breach brought attention to JavaScript's website vulnerabilities. The so-called "Skimming" or "Magecart attack" targeted finance-related data. British Airways is currently facing a £183M fine imposed by UK's GDPR watchdog, ICO.

- Magecart attackers inserted card-skimming scripts into the subscription website for the Forbes print magazine, bringing down the affected site not long after the issue was discovered.
- Another Magecart card-skimming code was implanted on the checkout and wallet page on Macy's payment portal. The malicious code is believed to have captured financial and other personal data submitted by customers, including names, physical addresses, ZIP codes, e-mail addresses, payment card numbers, card security codes, and expiration dates.
- Malicious code injected into a third-party Javascript of an advertising agency, Paris-based Adverline, targeted credit card information of online shoppers at European-based e-commerce sites. The attack was discovered by TrendMicro and RiskIQ researchers.
- Hackers have infiltrated into servers of at least seven online service providers to inject malicious code on thousands of websites. The first instances were found to be on Alpaca Forms and Picreel servers. The malicious code logged all user data entered into form fields, including information submitted on checkout pages, contact forms, and login sections.

Takeaway: An ecosystem map of CDN (Content Delivery Network) and the security perspective is a must. Black Kite is currently the only company that checks CDN security among security-rating service providers.

#4 Collections & Claim Processing for HealthCare

Healthcare is a major industry with a multitude of different players in the eco-system. As in other industries, healthcare organizations outsource many services to third parties, such as collections and claim processing services. HIPAA enforcement and fines hitting the news headlines reinforces that organizations need to be more careful about where PHI extends beyond their perimeters.

- A breach that occurred at the American Medical Collection Agency (AMCA) affected the major healthcare companies using AMCA's services and eventually some 20 million Americans. AMCA's breach led to the exposure of patient names, dates of birth, addresses, phone numbers, dates of service, providers, and balance information as well as credit card and bank information.
- Around 45,000 patients' records were compromised at Rush Systems for Health due to a claim-processing third-party vendor. While medical history was not disclosed, patient names, addresses, Social Security numbers, birth dates and health insurance information were exposed in the Rush systems breach.

Takeaway: Take HIPAA seriously. Keep track of where your PHI data extends. Beware of your business associates (a.k.a third parties) and revise your terms of agreements with these parties to meet HIPAA rules.

#5 Data Centers & Hosting Providers

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 misconfiguration of servers or cyber attacks expose sensitive data in these environments.

- Image-I-Nation Technologies, a third-party providing software and hosting services to Equifax, Experian and TransUnion were breached. The complex attack took place through unauthorized access to personal information in the software firm's database. The exposed data may have included Social Security numbers, names, dates of birth and home addresses.·
- The Plead malware, leveraging a MiTM attack, took aim on ASUS web storage software, ASUS's cloud storage service. The vulnerability puts the users of the cloud platform at risk.
- An unauthorized user accessed server in a data center that NordVPN was renting from an unnamed provider. This attack exposed some of the browsing habits of customers who were using the VPN service to keep their data private.

Takeaway: Discover all of the 3rd and 4th party service providers and cloud storage servers that your company uses. Check for misconfiguration of cloud storage servers Monitor cyber risk of your 3rd and 4th party providers

Leaky Bucket Syndrome

- CapitalOne had a data breach exposing around 140,000 Social Security numbers, 1 million Canadian Social Insurance numbers, and 80,000 bank account numbers. In addition to financially-sensitive data such as people's credit scores, credit limits, and balances. The breach occurred through an Amazon ex-employee who took advantage of a misconfigured Amazon bucket, where CapitalOne had kept its data.
- IPR, a PR, and CM company, also had some customers' data exposed due to a misconfigured Amazon bucket. Researchers discovered the bucket to be publicly accessible and that it included both IPR-related and customer-related sensitive information.

Other Third-Party Breaches

Flight Booking, OCR, Forum Site

- A flaw in a flight booking system was found to have potentially impacted *141 airlines and tens of millions of travelers* around the globe. By changing a parameter in the link using the PNR number, a hacker could see the booking information associated with other accounts. Frequent flyer miles could also be captured and moved to another account through this flaw.
- A misconfigured server of a third-party vendor, providing OCR services to financial institutions, exposed millions of bank loan and mortgage documents. The documents contained sensitive information for many major financial institutions including CitiFinancial, HSBC Life Insurance, Wells Fargo, CapitalOne and some U.S. government departments.
- Hackers have stolen almost 8 bitcoins ($28,200) from five victims through LocalBitcoins, a peer-to-peer cryptocurrency exchange portal. The breach was accomplished through a third-party service used in the exchange portal's forum sites.

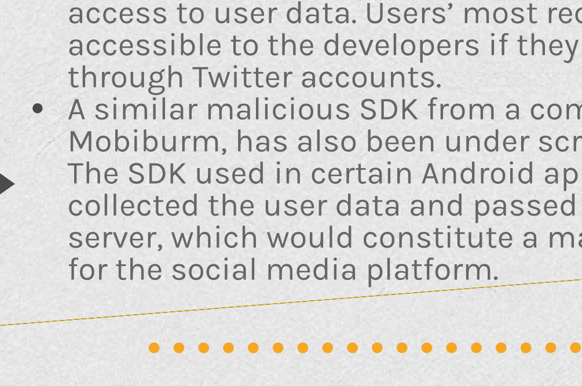
Third-Party Apps and SDKs

Facebook has and continues to remain under scrutiny by UK's watchdog ICO for data breach and privacy violations of user data by Facebook third-party apps.

- More than 540 million records of Facebook users were exposed including account names, IDs, passwords and user activity, through a third-party Cultura Colectiva. The records were found to be online on one of Amazon's publicly accessible cloud computing servers.
- A late-2019 compromise was discovered on Twitter due to a software development kit (SDK) called "One Audience". The SDK gave its developers unauthorized access to user data. Users' most recent tweets were accessible to the developers if they logged into the app through Twitter accounts.
- A similar malicious SDK from a company named Mobiburm, has also been under scrutiny by Facebook. The SDK used in certain Android apps may have illegally collected the user data and passed it to its central server, which would constitute a major privacy violation for the social media platform.

Third-Party Vendors & Service Providers

- Another platform called Houzz, allowing over 40 million users to log in through their Facebook credentials, was also hacked in 2019. The exposed information included, first name, last name, city, state, country, profile description, email addresses, IP address, and users' Facebook ID depending on their login choice.
- Atlanta-based family dining brand, Huddle House, had a POS-related breach over a two-year period due to a third-party. Criminals compromised the third-party point of sale (POS) vendor's data system to gain remote access and deploy malware to the Huddle House payment system. The breach is believed to have taken place beginning from August 1st 2017 through early 2019.



Record-breaking Fines & Record-breaking Exposure

Between January 2019 and December 2019, around 430 breaches were reported to HIPAA. Among them were some record-breaking third-party breaches exposing millions of patients' records. 2019 was also a year where the outcomes of some 2018 third-party breaches were resolved, as in the case of TicketMaster and British Airways breach. British Airways is struggling with a GDPR fine of £183M (although the fine is not final) for placing approximately 500,000 customers' personal information at risk; which does not take into account multiple class-action suits against the company.

Monitor your third parties

Quantifying the cyber risk of your third parties is extremely crucial to avoid data breaches caused by third parties. Risk quantification is a multi-dimensional problem. Black Kite provides a three-dimensional view to your third parties at scale.

3D Vendor Risk @ Scale

Cyber Rating

Perform non-intrusive cyber risk assessments of any third party. Get cyber ratings with easy-to-understand letter grades and drill down into technical details in each risk category.

Probable Financial Impact Rating

Use the FAIR model to calculate the probable financial impact if a cyber event were to occur at a third party in order to cost-effectively achieve and maintain an acceptable level of loss exposure.

Compliance Rating

Correlate findings to industry standards and best practices. Measure any third party's compliance with regulations and standards like NIST 800-53, ISO27001, PCI-DSS, HIPAA, GDPR, and Shared Assessments.

Request a free report

BLACK KITE

We regularly monitor third-party data breaches and provide a list at our website.

Visit www.blackkitetech.com to learn more about how to monitor 3rd-party cyber risk.