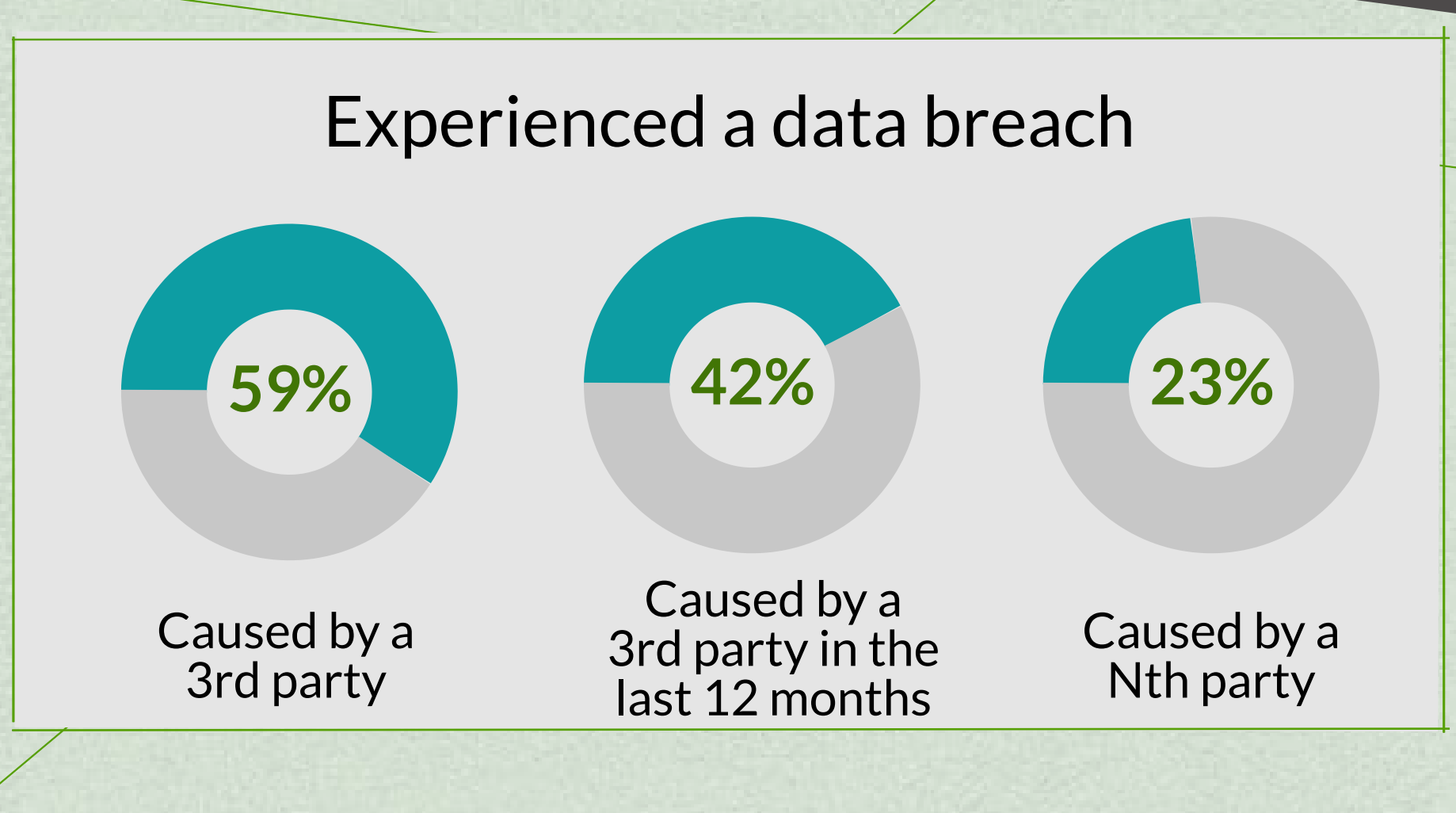
MAJOR 3rd-PARTY DATA BREACHES OF 2018

3rd-party (aka supply-chain) cyber attacks were one of the main reasons for major data breaches in 2018. Here is a recap of 3rd-party data breaches that hit the news in 2018

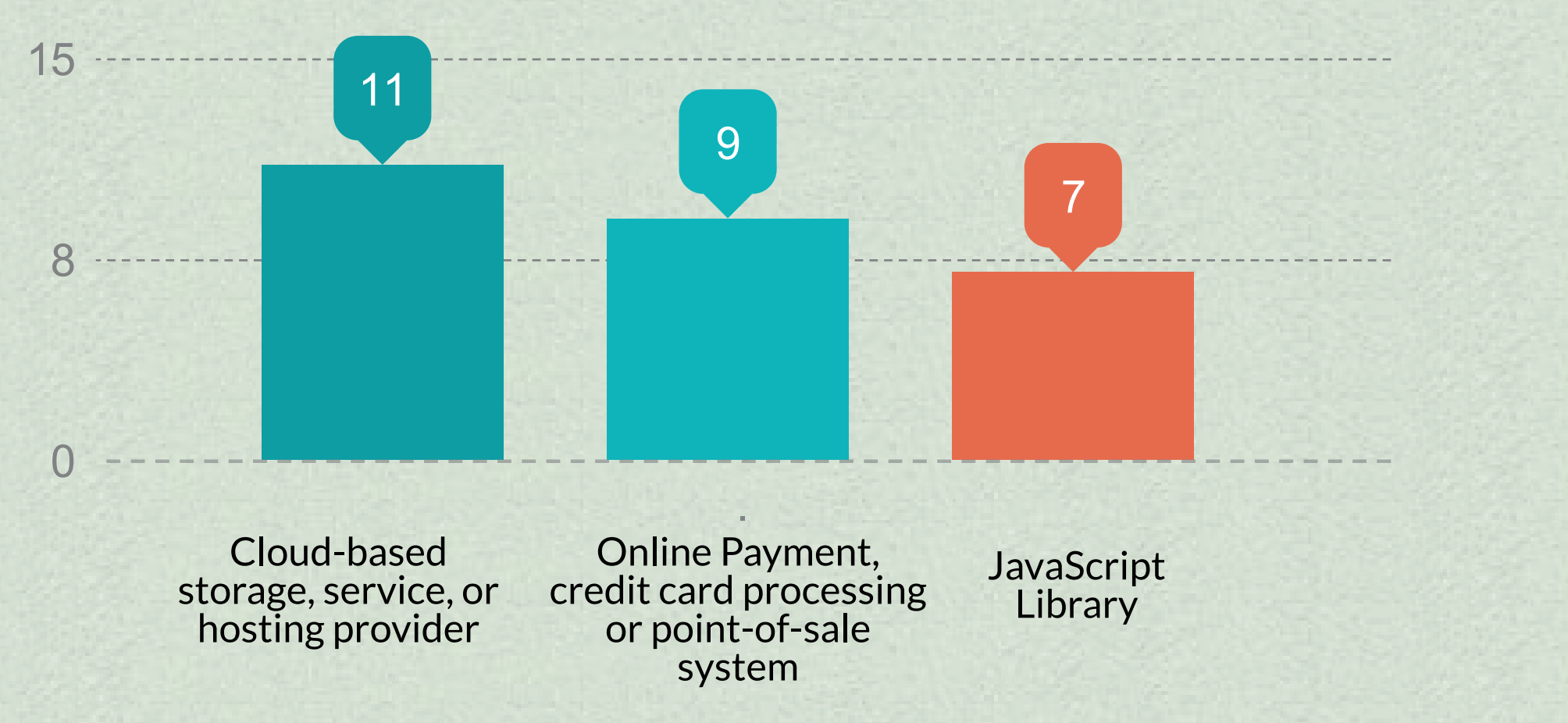
Almost 60% of the companies experienced a data breach caused by 3rd party

According to the 2018 Data Risk in the Third Party Ecosystem Study from Ponemon Institute


Experienced a data breach

Top 3 use of a third party

We reviewed 54 major data breaches caused by a third party and disclosed in 2018. Here are the top 3 uses by a third party.



Cloud-based storage, service, or hosting provider

Many companies use cloud services to store - sometimes sensitive- data and perform cloud-based applications. They also leverage hosting providers to manage their websites. Though cloud and hosting providers are usually secure, sometimes misconfiguration of servers or cyber attacks expose sensitive data.

- A misconfiguration of AWS S3 Bucket exposed 31,000 servers of GoDaddy, which contained sensitive data.
- A cyber attack on Agilisium (cloud data storage contractor) exposed system credentials and root passwords of Universal Music Group.
- Hacking IT Lighthouse (an application-hosting service provider) exposed 16,000 health information records of Redwood Eye Center patients.

Online Payment, credit card processing or point-of-sale system

Money is one of the top motivations of cyber criminals. So it is no wonder why they target payment systems.

- A cyber attack on cash register system operated by a third party provided unauthorized access to 165,000 Foosackly customers' paymentcard information.
- Hackers exploited a vulnerability in a payment system to pay parking fees operated by Click2Gov and used by more than a dozen cities in the US and Canada and managed to steal credit card information for more than 10,000 people.
- A health institution, Baylor Scott & White Medical Health in Texas, experienced a data breach caused by a third party responsible for operating a credit card processing system resulted in the breach of approximately 47,000 payment records.

Javascript Libraries

External Javascript, the code that resides in your website to track your visitors or gather analytics about them, are hidden third-party cyber risks that may cause severe data breaches.

- Magecart campaign, a series of card skimmer attacks, hit many large companies by injecting malicious code to Javascripts.
- Magecart's first target was a Javascript operated by Inbenta but run over TicketMaster's website. 40,000 users' information were exposed.
- Another major attack as a part of the same campaign was against British Airways, where credit card information of 380,000 customers were breached.
- A javascript managed by StatCounter to perform web analytics was hacked. This javascript was used by multiple sites, but attackers focused on gate.io, a cryptocurrency exchange, which ended up some bitcoin theft.

Online tools

Companies rely on online tools, such as chat bots or survey tools, to help run their main business. However, this reliance may may come with 3-rd party cyber attacks.

- A vulnerability of an online chat application was exploited by hackers. Companies that use the application such as BestBuy, Sears, Kmart, Delta, and others experienced massive data breaches with hundreds of thousands of customer records (per company) were exposed.
- Online employment services also caused data breaches in 2018. A cyber attack on an employment tool provided by JobScience, Inc. leaked Social Security numbers of thousands of applicants seeking for a job at El Centro Regional Medical Center in California and Huntsville Hospital in Alabama. There was another attack on PageUp's online recruitment services affected Whitbread.
- An online survey tool managed by TypeForm and used by Monzo, Adidas, TicketMaster, Harvey Norman, Fortnum & Mason, and more exposed millions of credentials.

Small- or mid-tier suppliers

Cyber risk of a supplier that you get some goods or a vendor with that you do business should be monitored closely. At the end of the day their cyber risk multiplies yours.

- A cyber attack to Invermar, a seafood supplier, cost the grocery chain Wegmans over $900,000.
- The fitness vendor of University of Louisville, namely Health Fitness Corp., caused data breach of personal information of hundreds of employees and retirees.

Mobile App Services

Some companies outsource mobile application services. Any vulnerability on a mobile app can result in the data breach of customer data.

- Hacking a mobile app externally developed for Air Canada exposed the data profile of many customers, which included personal and travel information.
- An attack on One Planet York mobile app developed by Appware for The City of York Council (UK) compromised almost 6,000 individual's personal information and credentials.

Transcription Services

Health institutions use transcription services managed by third parties. Attacks on those services may cause a data breach of patients, a situation which results in huge penalties under certain regulations such as HIPAA.

- Orlando Orthopaedic Center suffered such a data breach caused by a transcription-service provider and 19,000 patient records were exposed.
- An attack on Nuance Communication that provides transcription service to UC San Diego Health caused a data breach for hundreds of patients.

Marketing

The data shared with marketing firms to better understand the customers increase cyber risk.

- Mention, a company that offers brands, such as Airbnb, Microsoft, and Adobe, a media monitoring application, was hacked through a 3rd-party vendor used in its marketing stack. Potential data exposure included personal and account profile info (plan value, # of alerts and mentions).
- The cyber attack on Hova Health, a telemedicine company, left 2 million patient data, which probably belongs to a Mexican government health agency, exposed online.

Billing or Accounting Services

Accounting and billing operations can be complex and time consuming. Thus, using an external service makes sense as long as you understand the cyber risk it brings.

- Billing services provided by AccuDoc Solutions Inc. to Atrium Health was the target of a cyber attack and 2,65 million patient records were breached.
- A data breach caused by a third party used for the management of the direct deposit of wages by Nordstorm exposed personal and banking information.

Over a billion records breached in 2018

In 2018, over a billion records exposed cumulatively according to NordVPN.

- Facebook announced that more than 50 million users were compromised. This exposure also puts all platforms using Facebook-login feature under 3rd-party cyber risk.
- Personal information of around 500 million guests of Marriott Hotels is under risk of exposure. The data breach started at Starwood Hotels before Marriott acquired them. This incident shows the importance of due diligence during M&A operations.

NormShield

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

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