How CYE Calculates Cost of Breach

For those in charge of making decisions about their company's cybersecurity, quantifying monetary loss due to a data breach event (which we also refer to as "breach impact"), can be invaluable for the decision-making process.

Traditional Breach Impact Modeling

The typical standard for breach impact modeling is implemented mainly by insurers. Companies that sell cybersecurity insurance maintain their internal actuary models for estimating the insurance premiums and payouts for breached companies.

The main components of loss these insurers define are:

- Breach event containment costs
- Regulatory fines and class-action lawsuits

Containment costs apply to expenses like hiring a breach coach and establishing a call center, which are almost always estimated according to the organization's size and network complexity.

Many insurers predict the fines and lawsuits component based on a singular value: the number and type of personal private records expected to be leaked. They usually derive this information from the industry and number of the organization's (direct) customers.

A limitation of the number-of-records based approach is that a company may be liable for leaks connected to their products: For instance, an organization selling invoice management systems to retailers could be held accountable and even sued if the private data of these retailers' customers is leaked through the invoice system. This sort of "vendor impact" is often neglected by companies and insurers, who do not plan for this broad scope of loss.

Drawbacks

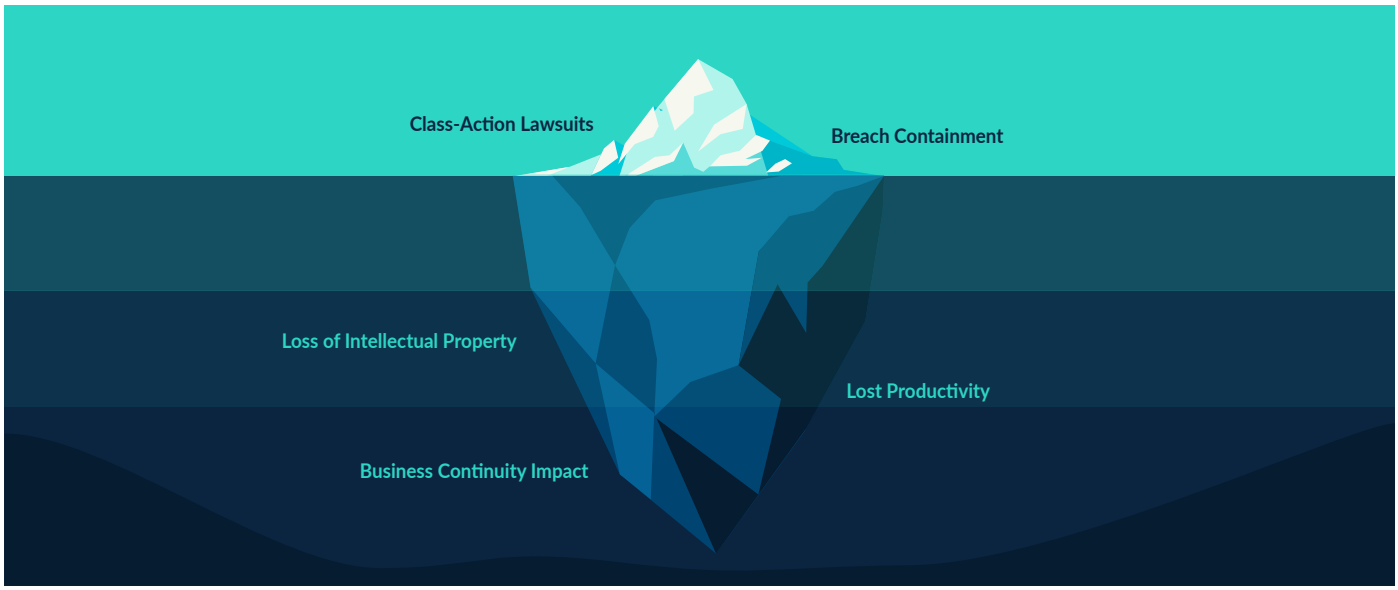
Although being the de-facto standard in breach impact estimation, cybersecurity insurers are far from being comprehensive and accurate:

- They lack the required intimate knowledge of the cybersecurity maturity level of the organization, its attack surface, vulnerabilities, and targeting information to correctly assess the likelihood of a breach event.
- They may miss significant parts of the loss, like the rising cost of ransom payouts, which is also linked to the cryptocurrency conversion rate.
- They only ensure the explicit parts of the loss — those related to containing the breach event and compensating victims. Other company losses are very conservatively estimated, if at all.

Ultimately, the bottom line is that relying on insurance companies to predict the full scope of loss can be problematic. The insurers are not really motivated to provide a comprehensive view of data breach loss. They limit themselves and the premiums they sell to tangible and provable expenses in well-defined categories. This may be satisfactory for covering the breach event itself, but is lacking from the perspective of decision-makers or investors interested in the long-term losses such an event may entail.

The Hidden Losses

Often, the losses you are insured for are just the tip of the iceberg.



Quantifying organizational losses beyond the immediate costs of containing the event and paying penalties and settlements requires identifying hidden loss components. These components relate to the revenue and productivity of the organization, and how these may be affected by a breach event. Here are some hidden loss components that CYE considers:

Brand Damage

A major loss factor which is not accounted for in a traditional breach impact estimation is reputation and brand damage. Many companies such as Equifax, which experienced a breach, subsequently suffered unprecedented losses.

The first and most easily quantifiable loss is in stock value. A reduced stock value translates to direct losses for investors and damages the organization's ability to raise capital through its stock. The stock performance is many times also an indication of lost revenue.

Equifax stock performance, compared to SNP500, in a one-year timeline containing the breach ((June 2017 – June 2018))

Customer churn can also lead to substantial losses. The Ponemon Institute reported an average 3.9 abnormal churn rate for companies that suffered data breaches in 2019, rising from 3.4 in 2018. It's important to note that the reported churn greatly varies depending on country and sector. Some countries like France or Japan can expect much higher churn rates (up to twice the churn of other countries). The industry where the organization operates is also key for predicting churn rates. Some industries like energy, utilities, or public (government) experience much lower churn rates than companies operating in more competitive industries like cybersecurity. These are only part of the factors that weigh into brand damage estimation.

An important caveat of brand damage estimation is that **companies do not always suffer stock loss and increased customer churn.** The security posture of the organization, and mainly how it is perceived by its customers and investors, is a major component in the outcome of a breach event, and specifically the effect on the company's brand.

Business Continuity & Productivity Loss

When a company suffers a breach event, systems go down—either directly by the actions of the hackers or by the company itself, which is trying to contain the event. Systems being down means that the company cannot generate any revenue from its online systems and that many employees are left idle for the duration of the event.

The canonical formula, therefore, that CYE uses for revenue and productivity losses is:

Loss = (Lost revenue per hour + Lost productivity per hour) * Downtime duration

The equation may seem simple; however, estimating each of its components is a formidable task. **Revenue and productivity per hour** can vary greatly depending on the organization in question, as the revenue and productivity dependency on systems uptime is different for each organization. CYE predicts these factors based on data aggregated by industry and country, while also allowing for the organization itself to provide these terms.

Downtime duration for a breached company depends on the type of company and mainly the level of skill of the employees tasked with containing the breach and getting systems back up, as well as the tools and policies put in place to mitigate such an event. Of the three terms of the loss formula, this part would be the hardest for the company to estimate by itself. It requires knowledge and experience of skilled cybersecurity IT and IR (Incident Response) personnel.

Intellectual Property (IP)

Data leaks aren't always about leaking private user records. An increasing number of hackers are now targeting intellectual property of the organization as another means of monetary gain and extortion. IP records can range from source code files to sensitive documents and even unreleased content in media organizations like Netflix or Sony.

The Ponemon Institute published several studies that identified lost IP as a potentially major factor of loss. According to the studies, companies are putting more emphasis on intangible assets (i.e., IP) as a major stream of revenue. Losing these assets can lead to major losses in the long term; for example, when leaked IP results in the loss of a competitive edge due to trade secrets, code, and algorithms being exposed.

The Decisive Factor: Exposure

Breach impact estimation is a powerful tool for decision making. It allows an organization to evaluate risk and budget cybersecurity spending correctly. However, it provides only part of the picture. To truly assess risk, the organization needs to evaluate *likelihood of breach*.

Consider the car metaphor: Losing a brand new $400,000 Ferrari 599 GTO would cost you $400,000 — but that's not the risk. Risk also depends on the road conditions in your city and how well you drive, meaning, the probability of an accident.

The same is applied for data breaches. The exposure of an organization depends on its cybersecurity standing and the likelihood of it being hacked, as well as its breach impact, and specifically:

Exposure = Likelihood of breach x Impact of breach

Case Studies

Here are examples of how CYE determined the cost of breach for simulated companies from three different sectors: technology, healthcare, and financial.

Financial Company

The financial company is a young fintech company founded in 2016 and located in the US. It has about 100 employees and an annual revenue of $10M.

PII/PCI/PHI

The company holds PII about its customers and especially PCI, since it handles credit card information.

IP RECORDS

It has very few IP records (20) and therefore, the cost of the lost IP is quite low compared to the other first-party costs.

ABNORMAL CHURN

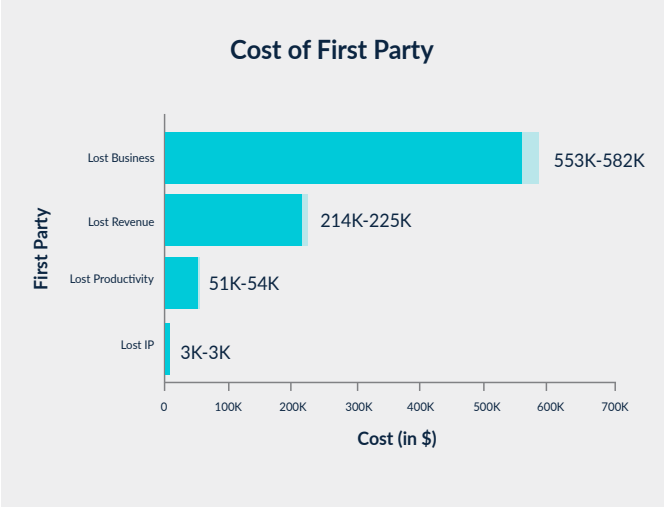
Considering the industry (finance) and location (US) of the company plus the security posture (low, since the company is young), the predicted churn is 5.5%.

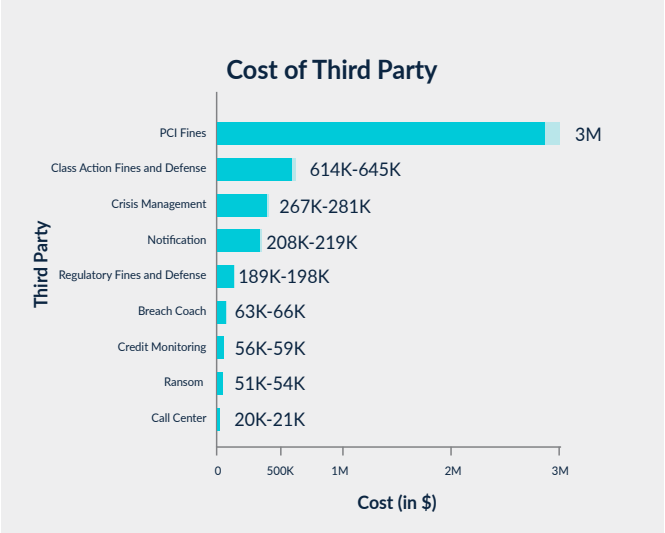
DOWNTIME

The estimated downtime is 16 days, since the security posture of this young company is yet to be improved, which explains here why lost revenue is relatively high. In addition, the uptime dependence for the productivity and revenue is factored in at 40-50%.

RANSOM

The ransom is low relative to other costs, considering the size of the business and number of employees.





Total cost of breach: $5.1M–$5.4M

Medical Company

The medical company is a 10-year-old HealthTech company founded in 2016 and located in France. It has about 2,500 employees and an annual revenue of $300M. They sell medical devices for the hospitals, private doctors, and individuals ($50M customers).

The company sells to real people, and they can be held liable for the number of “extended customers” (e.g., final customers).

PII/PCI/PHI

The company holds PII about its customers and especially PHI since it handles health information. Therefore, it has no PCI fines, but is liable for regulatory fines and defense, class action fines, and defense costs.

IP RECORDS

It has 15,000 IP records, since it is a medical company with a lot of patents. The cost of lost IP records is therefore more consequential here: 13% of the first-party cost.

ABNORMAL CHURN

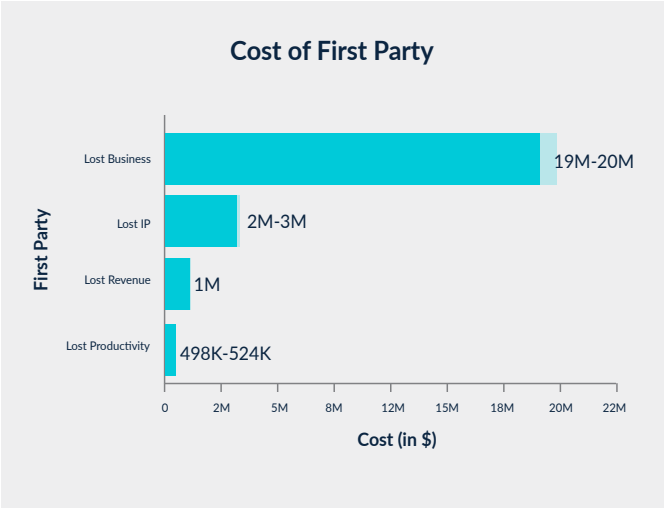
Considering the industry (medical) and location (FR) of the company plus the security posture (medium), the predicted churn is 6.4%.

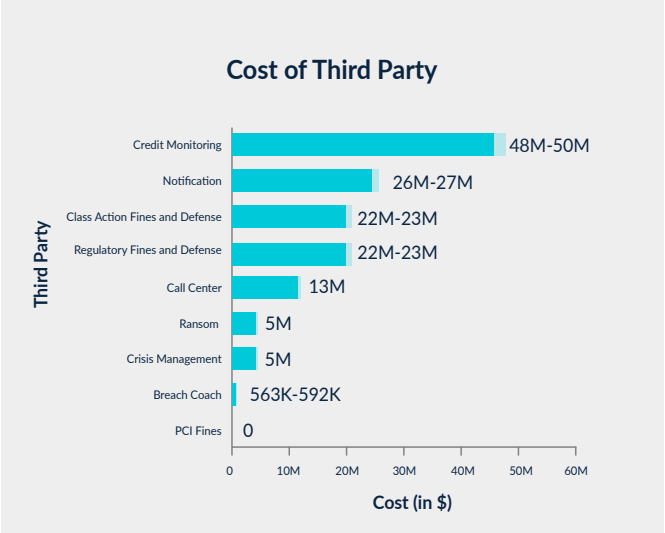
DOWNTIME

The estimated downtime is two days. The uptime dependence for the productivity and revenue is 70-75%.

RANSOM

The ransom reaches a maximum value of observed ransoms to date ($5M).





Total cost of breach: $164M - $172M

Technology Company

The tech company was founded in 1997 and is in the US. It has about 50,000 employees and an annual revenue of $12B. It has a wide range of products related to the internet and the cloud with over 100M clients worldwide. It has a SOC, security analytics, DLP (data loss prevention plans) and Red Team testing.

The data breach that would occur would be a “mega-breach” (>1M records). The company has very few competitors since it has a monopoly over its industry. Users are locked in with a few options.

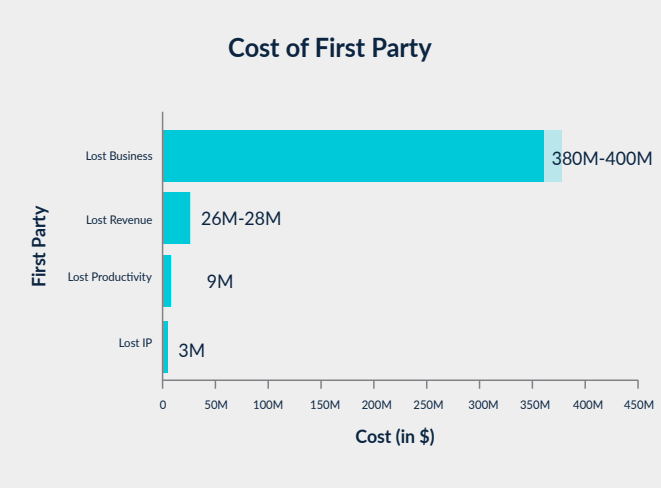
PII/PCI/PHI
The company holds only PII about its customers.

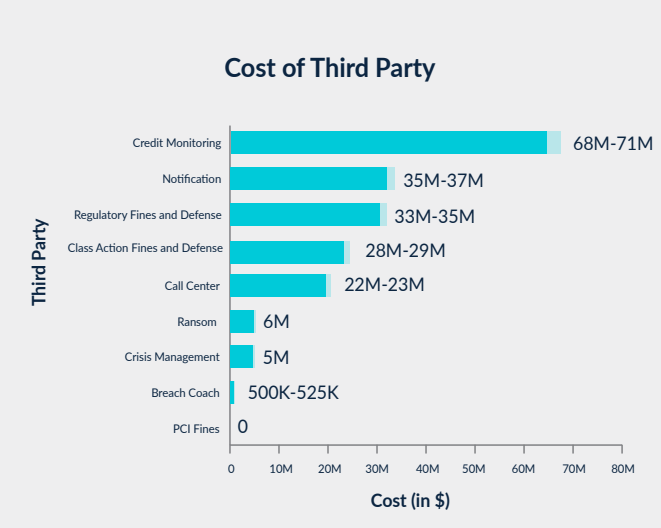
IP RECORDS
It has 20,000 IP records. The cost of IP lost IP records is estimated to be $3M, which accounts for little compared to other costs in this case.

ABNORMAL CHURN
Considering the industry (tech) and location (US) of the company plus the security posture (high), the predicted churn is 3.3%.

DOWNTIME
The estimated downtime is less than a day. The company has a security posture considered high. The uptime dependence for the productivity and revenue is 100%.

RANSOM
The ransom reaches a maximum value of observed ransoms to date ($5M).



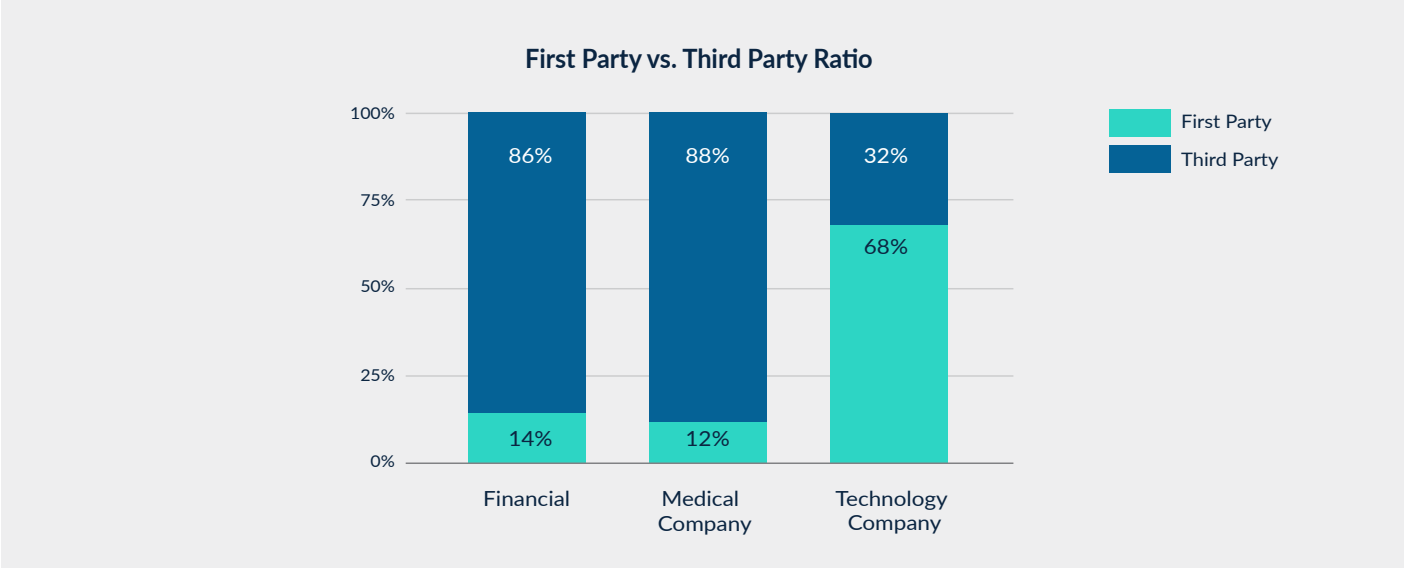


Total cost of breach: $615M - $647M

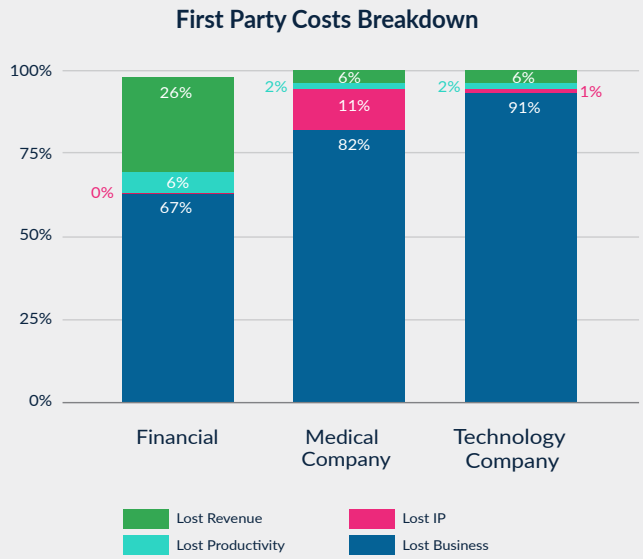
Comparison Between the Cases

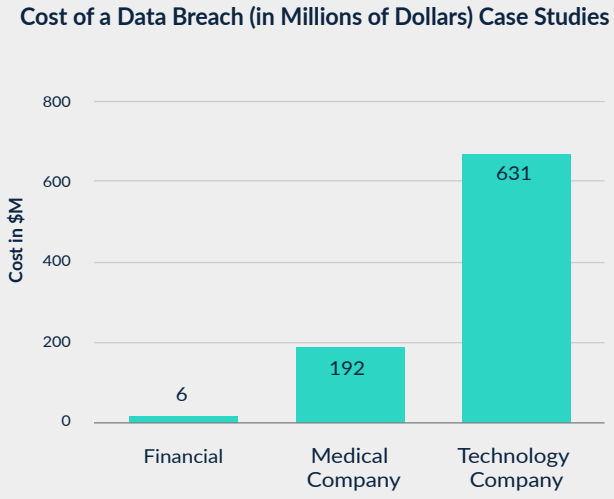
While there are similar ratios of first-party and third-party costs between the medical and financial companies, the technology one has a much higher ratio of first-party costs. This can be explained by the following:

- The advanced security posture of the technology company lowers the third-party costs considerably.
- The technology company is completely dependent on its online systems for its productivity and revenue, which increases the first-party costs in case of a data breach.



Since the medical company has many IP records (compared to its revenue), we notice that it accounts for a good part of the first-party costs. Also, the financial company has a high ratio of lost revenue due to its very high downtime since its security posture should be improved.





Sources and Methodology

CYE's Breach Impact model is based on data collected internally by CYE's security researchers and incident response specialists and reflects years of experience and intimate knowledge of the cybersecurity landscape and breach events. This data is combined with breach statistics collected over years from hundreds of breach events in companies, spanning various industries and countries, supplemented by public sources and studies.

ABOUT **CYE**

CYE's optimized cyber risk quantification platform and expert guidance transform the way organizations manage cybersecurity. Using AI, machine learning, and innovative technology, CYE visualizes attack routes, quantifies, mitigates, and communicates cyber risk, and matures organizational cybersecurity posture. In doing so, CYE provides clear and relevant insights that empower companies to make effective cybersecurity decisions. The company serves organizations in multiple industries globally. Founded in 2012, with headquarters in Israel and operations around the world, CYE is funded by EQT Private Equity and 83North.
Visit us at cyesec.com.

Want to learn more about how CYE can help protect your company from cyber threats?

Contact us