CYE

Inadequacies in Breach Insurance Coverage: A Data-Driven Gap Analysis

Insurance As a Cyber Risk Reduction Tool

In an era where digital threats loom larger than ever, businesses are increasingly turning to cyber insurance as a safeguard against the financial ravages of data breaches. Yet CYE's study leveraging external and internal datasets reveals a stark reality: the protection afforded by such insurance may fall significantly short of the actual costs incurred during cyber incidents. This report delves into the depths of cyber exposure management, unearthing the critical coverage gaps that threaten organizational stability in the wake of cyberattacks.

Key Findings: The Coverage Gap Exposed

Cyber Insurance Coverage

80% of insured companies that suffered a data breach did not have sufficient coverage.

Average Coverage Gap

The average coverage gap is **350%,** meaning that more than 3/4 of the incident was not covered. This translates to **$27.3M** average uncovered loss.

Maximum Coverage Gap

In some cases, the maximum coverage gap reached **3000%**.

Revenue Impact

The coverage gap accounted for **2.9%** of revenue when removing outliers. With outliers, the coverage gap is **42%.**

Sectors Affected

"Low tech" sectors of accommodation and food services, construction, transportation and warehousing are among the more adequately covered ones, while sectors like finance and insurance, information and manufacturing present well beyond a **100% gap** in coverage on average.

Insurance Gap Trend

The general insurance gap trend did not decline in recent years. This suggests a gap in organizations' ability to accurately quantify their risks, and a gap in the ability or willingness of cyber insurers to provide adequate insurance coverage.

Visualizing the Data: A Closer Look

Figure 1 reveals the entire picture. It divides all reported cyber insurance cases into categories:

- Adequately insured companies: 20% of cases
- Small (<50%) gap in insurance: 20% of cases. Average gap: 22%
- Between 50% <100% gap: 23% of cases. Average gap: 74%
- Between 100% <200% gap: 16% of cases. Average gap: 151%
- Huge (150% <500%) gap: 12% of cases. Average gap: 423%
- Astronomical (500% <3000%) gap: 7% of cases. Average gap: 2464%

A staggering 35% of cases suffered inadequate coverage of over 100% (more than twice) of the breach costs.

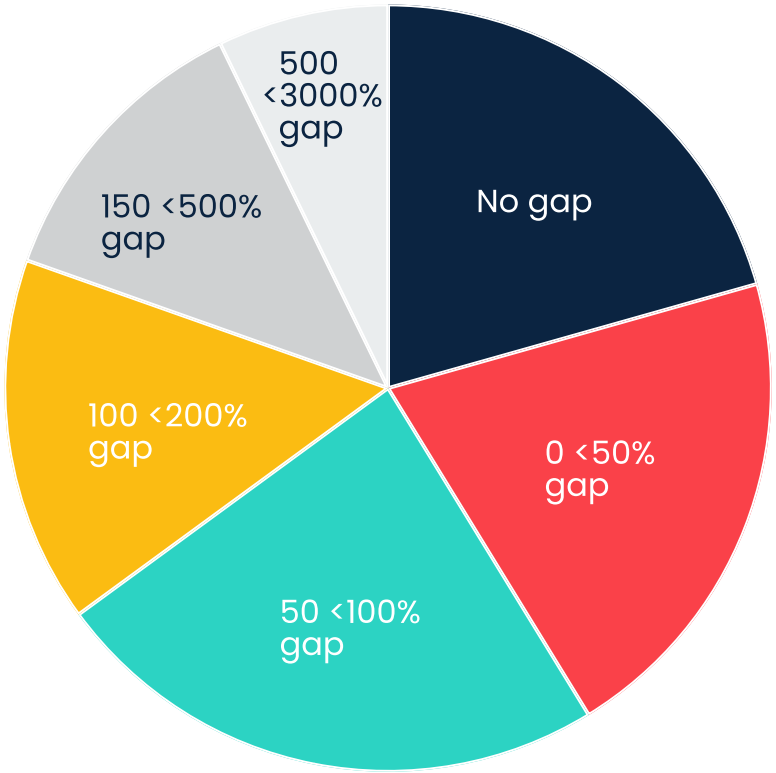


Figure 1: An overarching view of coverage gaps across all analyzed sectors.

Insurance Gap by Sector

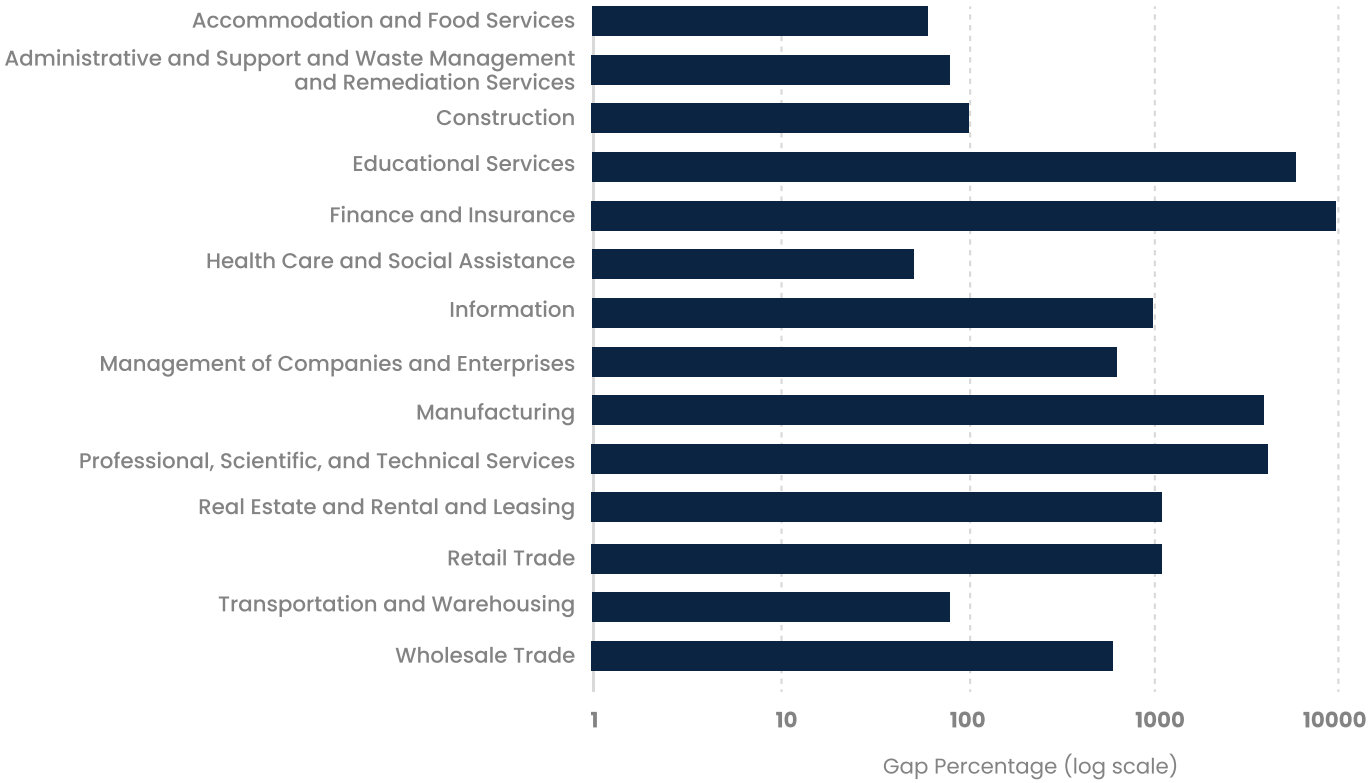


Figure 2: Insurance gap by percentage, per sector

Figure 2 depicts the average insurance gap of different sectors. Among the more adequately covered industries, we can find the "low tech" sectors of accommodation and food services, construction, and transportation and warehousing. Meanwhile, sectors like finance and insurance, information, and manufacturing present well beyond a 100% gap in coverage. This figure, although surprising, can be explained by the fact that companies in the latter sectors have more digital assets and are more dependent on digital systems to operate. Moreover, in many cases, these companies are unable to acquire full adequate coverage due to the astronomical potential price of a breach in their sector. These organizations are left with no choice but to shift their focus toward risk quantification to efficiently reduce risk that cannot be covered.

Uncovered Losses as Percentage of Revenue

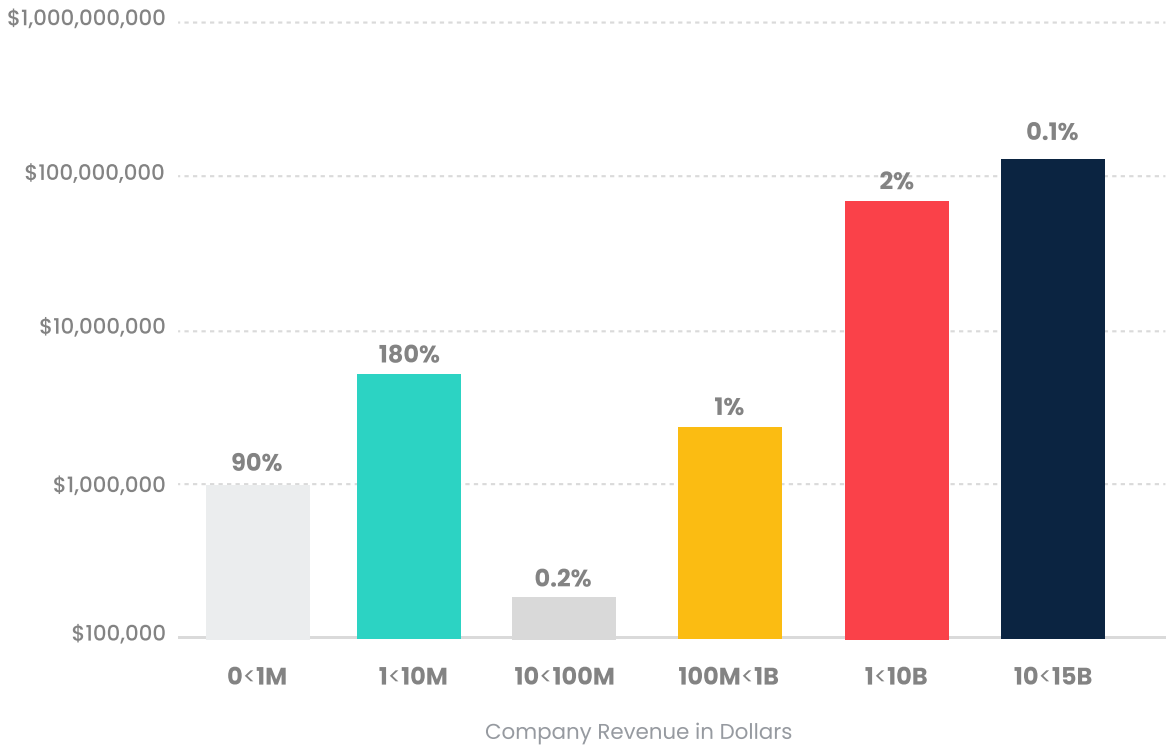


Figure 3: Uncovered losses as percentage of company revenue

Figure 3 describes the average uncovered loss as a percentage of the company revenue, by category of revenue. An important and actionable insight here is that inadequate coverage is a high risk for small companies with less than $10M in revenue.

In cases of bootstrapped companies, with no large investments backing them, an uncovered breach can be a death blow that effectively ends company operations. These types of companies should exercise extreme caution with their cybersecurity hygiene or make sure they have sufficient coverage.

Insurance Gap Over Time

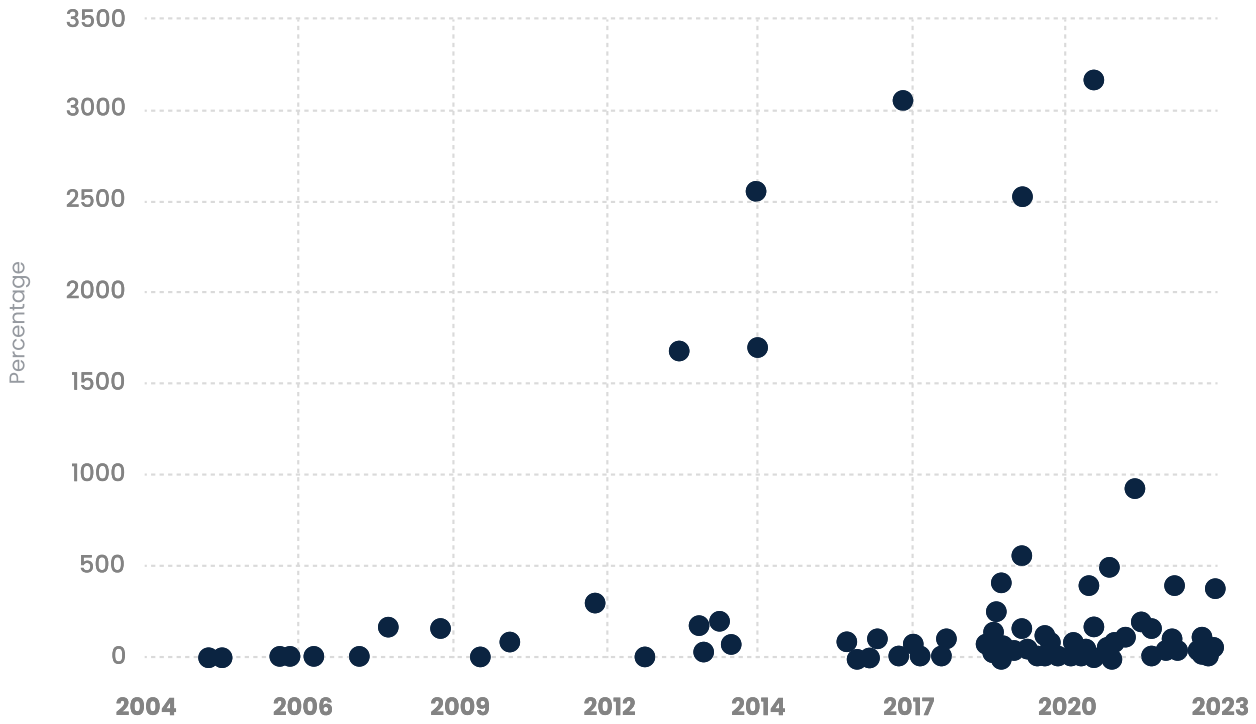


Figure 4: Insurance gap (uninsured cost/insured cost) as time progresses.

Figure 4 describes the insurance gap as a function of year of event. Two major insights can be drawn from the data:

1. Outlier events (cases where uninsured costs percentage are in the thousands) exacerbate over time, as can be seen in the data points above the 1000% mark.
2. The general insurance gap trend does not decline. It's important to note that events up to 2012 may seem as if insurance was adequate in past years, but this is most likely due to reduced reporting capabilities, and that cybersecurity insurance was less prevalent in those years. Ultimately, we are not seeing improved capabilities in estimating breach costs as time progresses, as the gap remains in the tens and even hundreds of percents. This suggests a gap in organizations' ability to accurately quantify their risks, and a gap in the ability or willingness of cyber insurers to provide adequate insurance coverage.

Case Studies: Breaches Under the Microscope

Finance and Insurance Sector:
Orrstown Bank's Ordeal and Capital One

In a striking incident in April 2019, Orrstown Bank suffered a breach resulting in a tug-of-war with its insurer over a claim of approximately $765,000 in response efforts, only to receive a partial reimbursement. The insurer denied the full claim, leaving the bank with an uninsured exposure of $279,000 against its insured coverage of $486,000.

On a much larger scale, on July 29, 2019, Capital One, based in the US, reported a significant security breach where an external party gained unauthorized access to the personal information of 106 million credit card applicants and customers. This breach was due to a configuration vulnerability in Capital One's infrastructure. Subsequently, the FBI, as announced by the US Department of Justice, arrested the hacker responsible for this intrusion.

Capital One estimated the financial impact of this breach to be $138 million, covering costs for customer notifications, credit monitoring, technology updates, and legal support. Despite receiving $73 million from insurance, the company faced $65 million in uncovered damages. This event highlights the substantial repercussions of cybersecurity breaches on companies, particularly when insurance does not fully cover the resultant financial losses.

Information Sector:
SolarWinds' Cyber Siege

The SolarWinds cyber incident, identified in December 2020, resulted in significant financial costs due to a sophisticated malware attack. The costs associated with investigation, remediation, and legal services were partially offset by insurance coverage, but a gap remained between the total expenses and the insurance payouts.

- **Through 2020:** Initial costs were $3.485 million, with subsequent reports indicating escalating expenses.
- **2021:** Expenses totaled over $49 million, with insurance covering about $16 million.
- **2022:** The company faced $56.4 million in gross expenses, offset by $30.2 million from insurance.
- **First quarter 2023:** Incurred an additional $2 million for response costs.
- **By September 2023:** Reported expenses were $15.5 million, with insurance proceeds of $19.8 million, an atypical period where insurance proceeds exceeded expenses.

In summary, while insurance provided significant relief, SolarWinds bore a substantial financial burden due to the cyber incident, reflecting the challenge of fully compensating for such breaches through insurance alone.

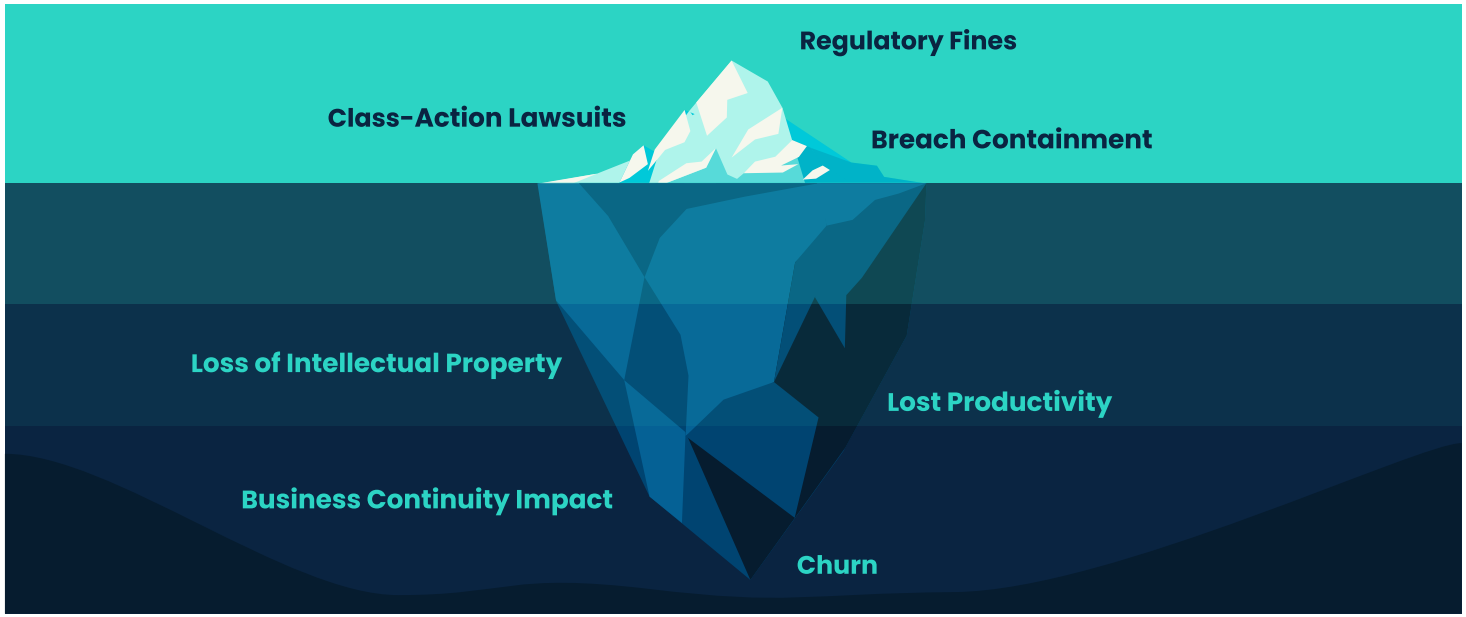
Manufacturing Sector:
Demant Cyber Incident

Demant, a Denmark-based manufacturer of Oticon hearing aids, experienced a significant ransomware attack in early September 2019 that disrupted its IT infrastructure. This attack affected several aspects of Demant's operations, including ERP systems, production, and distribution facilities in Poland and Mexico, cochlear implant production in France, amplifier production in Denmark, and several offices in the Asia Pacific region.

Despite the severe impact on its operations, there were no indications that personal data, including protected health information, consumer data, or private financial information, was accessed by the attackers. The company took immediate action to contain the breach by shutting down IT systems across multiple sites and business units, which allowed them to gradually resume business operations.

The financial consequences of the cyberattack were substantial, with Demant estimating losses up to $95 million. These losses included service disruptions, recovery costs, extra pay for IT staff involved in investigating and containing the incident, as well as expenses for new hardware and software. The company received a $14.69 million recovery from its cyber insurance coverage to aid in restoring its data infrastructure. However, the incident led to considerable financial strain beyond what insurance was expected to cover, leaving the company bearing the lion’s share of the expenses.

The Urgent Need for Accurate Cyber Risk Quantification



Remember: Breach events hide costs that may exceed direct costs dramatically

The findings underscore a pressing need for businesses to refine their approaches to cyber risk quantification. The prevailing underestimation of cyber risks leads to insufficient coverage, exposing companies to substantial financial vulnerabilities post-breach.

Companies need to remember that:

- Insurance companies can't (or won't) cover very high risks
- Covered risks almost never account for business risks like churn and loss of business continuity

Conclusion: Bridging the Cyber Insurance Coverage Gap

This study, grounded in CYE's extensive dataset, highlights the need for accurate cyber exposure management practices. As the digital threat landscape continues to evolve, so must strategies for mitigating financial risks. Accurate risk assessment and optimized mitigation emerge as indispensable tools in the arsenal against cyber threats, helping businesses navigate the digital age with confidence and security.
The journey towards comprehensive cyber risk coverage is complex, but with diligent analysis, strategic planning, and ongoing adaptation, businesses can safeguard their assets against the ever-growing tide of digital threats.

Data and Methodology

Drawing from an extensive pool of internal and external data breaches recorded in our dataset, this study analyzed a total of 101 incidents across various sectors containing breach coverage figures. The focus sharpened on sectors notably vulnerable to cyber threats: finance and insurance, manufacturing, and information. Through meticulous examination, the analysis revealed the disparities between insured and uninsured exposures, offering unprecedented insights into the financial aftermath of cyber incidents.

Want to learn more about how your company can accurately quantify its cyber exposure? **Contact us.**

About CYE

CYE's exposure management platform, Hyver, transforms the way security teams protect their organizations. With CRQ at its core, the platform reveals enterprises' exposure in financial terms, visualizes the most exploitable attack routes to critical business assets, and creates mitigation plans tailored to each business. CYE's customized reporting enables the sharing of vital board-level metrics and validating exposure reduction over time. In addition, CYE improves cybersecurity maturity by mapping weaknesses and defining targets based on industry frameworks. Founded in 2012 in Israel with operations around the world, CYE has served hundreds of organizations across industries globally.
Visit us at cyesec.com.

1000 North West Street, Suite 1410, Wilmington DE 19801, United States
1 Ballards Lane, London N3 1LQ, UK | Abba Eban 10, Herzliya 4615200, Israel