DATA SHEET

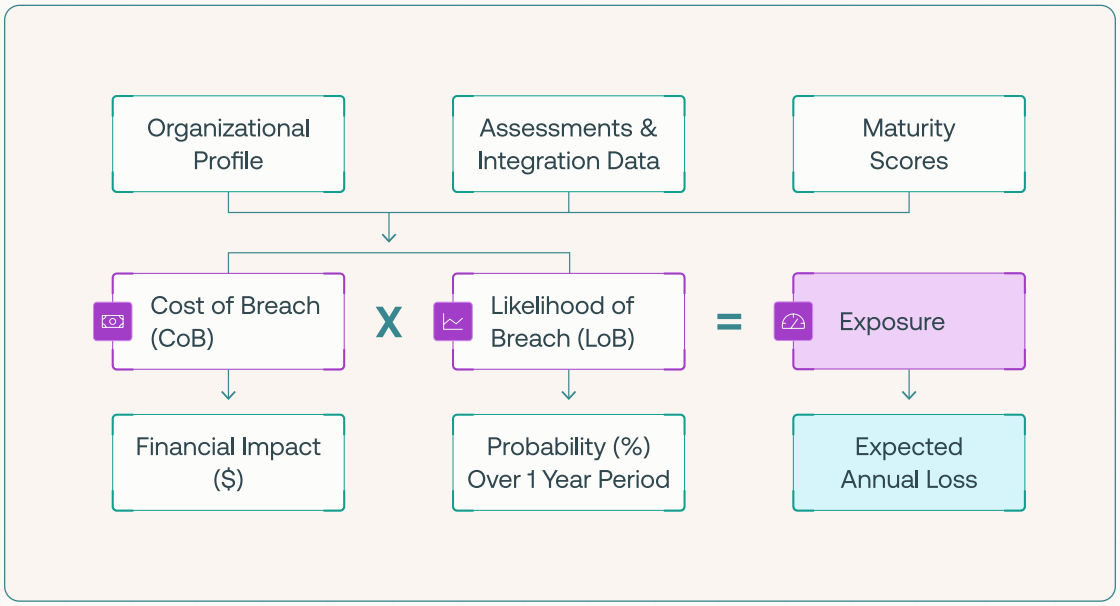
Cye **Exposure Management** Platform

Quantifying Cyber Risk with a Data-Driven Framework

Cye's exposure management platform uses cyber risk quantification (CRQ) to reveal exposure in financial terms, visualize attack routes to critical business assets, and prioritize mitigations that deliver the greatest expected loss reduction.

The **Quantitative Model** Behind Cye's Cyber Risk Calculations

Cye's platform applies actuarial science to cybersecurity by translating an organization's technical posture into financial risk metrics that executives, risk, and compliance leaders can trust. The model combines empirical breach data, actuarial datasets, and attack-path simulations to quantify both the likelihood and impact of cyber events. At its core, the platform integrates three actuarially aligned models - Cost of Breach (CoB), Likelihood of Breach (LoB), and Exposure (Loss Expectancy) - into a single coherent framework:



These figures are evidence-based, auditable, and regulator-defensible. Every output can be traced back to measurable inputs, actuarial datasets, or maturity-derived probabilities.

Core Components of the Platform

Model	Primary Objective	Data Inputs	Analytical Techniques	Risk Metric Delivered
Cost of Breach (CoB)	Estimates financial impact per BusinessCritical Asset	Advisen & Ponemon datasets, CYE incident data, maturity scores, business profile	Machine Learning, regression, actuarial calibration	$ Expected loss per breach
Likelihood of Breach (LoB)	Measures probability of attacker reaching an asset	Mitigation graph, exploit data, threat intelligence, Cye and external benchmarks	Graph theory, Monte Carlo simulation, benchmark calibration	% Probability of compromise
Exposure	Computes expected loss (frequency × magnitude)	Derived from CoB × LoB	Statistical aggregation, Bayesian inference	$ Annualized loss expectancy

Cost of Breach (CoB)

Cye uses an actuarial model to estimate the financial impact of a breach by asset type, covering regulatory fines, downtime, legal costs, and brand damage.

The model is trained on more than **250,000 verified breach records** and over a decade of Cye's proprietary red-team and incident-response data.

Inputs include business parameters like the organization size, geography, revenue, industry, etc. Along with the cybersecurity maturity posture as measured in Cye, in the NIST CSF format.

The model is trained on more than 250,000 verified breach records and over a decade of Cye's proprietary red-team and incident-response data.

Accuracy

The CoB model achieves an R^2 value of 0.93, which indicates a high level of accuracy. R^2 measures how much of the real-world variation in breach costs can be explained by the factors used in the model. A value of 0.93 means that 93 percent of the differences observed in actual breach costs are accounted for by the model's inputs, leaving only seven percent attributable to noise or unmeasured factors. This level of explanatory power is considered strong in statistical modeling and demonstrates that the model closely reflects the underlying cost drivers.

Example

Predicting breach cost with an R^2 of 0.93 is similar to predicting the weight of a package using its size and contents and getting almost the same number as the real weight each time. The model reliably follows the true drivers, which is why an R^2 this high is viewed as evidence of accuracy.

Likelihood of Breach (LoB)

LoB quantifies how likely it is that an attacker could reach a Business-Critical Asset (BCA).

Cye ingests the organization's assets and vulnerability data to build a Mitigation Graph and runs Monte Carlo simulations to test millions of potential attack paths.

Key Inputs

- Exploitability and availability of public exploits
- Threat intelligence frequency and active campaign data
- Historical red-team and breach-assessment results from Cye's global engagements
- Security maturity and compensating controls

Benchmarking & Validation

The LoB model is calibrated using Cye's benchmark dataset, derived from thousands of real-world assessments, and validated against external references such as the World Economic Forum, ENISA, and leading cyber insurance benchmarks.

This keeps the probability ranges data-grounded and aligned with globally recognized risk baselines.

Flow Attack Surface → Mitigation Graph → Monte Carlo Simulation → Likelihood (%)

Exposure (Loss Expectancy)

Exposure represents the statistically expected financial loss over time.

It is the metric that boards, regulators, and auditors can directly compare to expected-loss models in insurance and finance.

Cye continuously recalculates exposure as new vulnerabilities are discovered and mitigations are implemented, providing a dynamic, data-backed view of an organization's cyber exposure.

Formula

$$\text{Exposure} = \text{Likelihood} \times \text{Cost of Breach}$$

Why **Cye's Risk Metrics** Stand up to Scrutiny

Pillar	Explanation
Data-driven foundation	Based on 250K+ breach events, actuarial records, and Cye's proprietary field intelligence from global engagements.
Actuarial methodology	Uses proven quantification techniques including Monte Carlo simulation, Machine learning methods and ground truth calibration.
Benchmark calibration	LoB is tuned using Cye's assessment dataset and validated with external benchmarks such as WEF, and ENISA.
True-to-source modeling	Reflects real attacker behaviour and breach mechanics rather than static control checklists or theoretical assumptions.
Explainable outputs	Every metric is traceable back to its underlying inputs, visible in Cye's Mitigation Graph.
Regulator-ready transparency	Follows a frequency × magnitude approach consistent with CRQ and FAIR-style models, grounded in empirical data and suitable for audit and regulatory review.

Frequently Asked **Questions**

Q1. How are Cye's numbers validated?

Each model is benchmarked against verified actuarial and breach datasets (Advisen, Ponemon, Cye incident data, insurance records). The CoB model explains over 90% of observed cost variance, and the LoB model is cross calibrated using Cye's proprietary benchmarks as well as global references such as WEF and ENISA.

Q2. What makes this model defensible to auditors and regulators?

Cye's calculations are transparent, data-driven, and actuarially structured. Each figure stems from measurable inputs, documented data sources, and reproducible logic. The structure follows actuarial conventions commonly used in financial risk management and model validation.

Q3. Why trust Cye's estimates over other frameworks (e.g., FAIR or insurance calculators)?

Other models often rely on simplified proxies like record counts or revenue multiples. Cye integrates actuarial datasets, attack-simulation data, and organizational maturity to a comprehensive model, encompassing all risks and capturing both probability and impact from a realistic attacker perspective.

Q4. What role does maturity scoring play in these numbers?

Maturity data directly affects both likelihood and cost. Improvements in containment, detection, and recovery maturity reduce expected loss and provide a measurable link between security investment and financial risk reduction.

Q5. How should these results be interpreted by executives and risk committees?

Cye's outputs represent expected loss, not worst-case scenarios. They help prioritize mitigations, justify cybersecurity budgets, and align insurance coverage. The result is a transparent, regulator-credible translation of cyber risk into financial terms.



What this means for your organization

Cye's actuarial engine provides a quantifiable, auditable, and transparent view of cyber risk, enabling organizations to justify cybersecurity investments, satisfy governance and regulatory expectations, and demonstrate measurable reduction in exposure over time.

About Cye

Cye combines an AI-native exposure management platform with world-class cyber expertise to help organizations know the financial impact of their cyber exposure, prioritize risk mitigation and automate remediation. Cye's 500+ customers gain the clarity to make smart defensible decisions that reduce their risk exploitability with speed, and improve their resilience to the hyper dynamic threat landscape.

Visit us at cyesec.com.

© 2026 Cye, All rights reserved. www.cyesec.com | info@cyesec.com