Binary³ Risk Quantification Engine

Cybersecurity Threat Management & Gross Revenue Margin Impact

RESEARCH WHITE PAPER | RQE Financial Methodology | v2.0 | May 2025

Executive Summary

This white paper presents a rigorous, actuarially grounded framework for quantifying the financial impact of cybersecurity threats on gross revenue margins. The Binary³ Risk Quantification Engine (RQE) operationalizes this framework through a programmatic API, converting raw security findings into dollar-denominated risk scores that finance and security leadership can act upon directly.

This version extends the foundational model with five critical improvements: explicit program effectiveness parameterization, a Poisson alternative for probability annualization, Net Present Value discounting for program cost, tail-risk supplementation via Monte Carlo simulation, and multi-vector attack summation guidance. Together these bring the model to an institutional-grade standard suitable for insurance underwriting, M&A due diligence, and board-level risk reporting.

1. Theoretical Foundations

The algorithm draws from three established disciplines: actuarial risk science, financial engineering, and information security risk management.

1.1 Expected Loss Framework (EL)

In actuarial science, the expected loss of a discrete adverse event is the product of its probability of occurrence and its conditional loss magnitude:

```
EL = P(event) x Loss | event
```

RQE extends this by decomposing Loss into direct and indirect components, and deriving an annualized probability from multi-year threat frequency data, mirroring standard actuarial practice for low-frequency, high-severity operational events.

1.2 FAIR Ontology Alignment

The FAIR model (Open Group Standard C20B) decomposes risk into Loss Event Frequency (LEF) and Loss Magnitude (LM). RQE maps directly to this ontology: Annual Probability of Attack corresponds to LEF, and Total Cost of Cyber Attack to LM. This alignment ensures RQE outputs are compatible with enterprise risk registers and board-level reporting frameworks.

1.3 Limitations of Single-Point (Deterministic) Models

A deterministic expected loss calculation produces a mean estimate only. It does not capture variance, tail risk, or confidence intervals. For enterprise decision-making, Monte Carlo simulation over the loss distribution is strongly recommended. RQE's Exposure Modeling module implements this via parametric log-normal loss distributions, which are well-supported in the cyber insurance actuarial literature.

2. The Five-Step Financial Impact Algorithm

The following five steps constitute the core deterministic calculation exposed by the RQE API. Each step includes formal notation, variable definitions, key assumptions, and identified limitations.

Step 1 | Total Cost of Cyber Attack (TC)

The total cost represents the full economic impact of a single cyber attack event, partitioned into directly invoiced costs and costs that manifest as foregone revenue or value destruction.

Formula:

```
TC = C_d + C_i
```

Variable	Definition	Calibration Guidance
`TC`	Total Cost of Cyber Attack ($)	Calculated
`C_d`	Direct Costs: incident response, forensics, legal fees, regulatory fines, breach notification	IBM Cost of a Data Breach Report; Verizon DBIR average by industry
`C_i`	Indirect Costs: lost revenue, reputational damage, customer churn, productivity loss	Ponemon Institute; Gartner. Apply 1.4x-1.6x multiplier if directly unobservable

Assumption: C_d and C_i are treated as point estimates. Both are stochastic in practice. Indirect costs are routinely underestimated by 40-60% in post-incident analyses (Ponemon, 2023). A conservative 1.5x multiplier on C_i is recommended when direct measurement is unavailable.

Step 2 | Annual Probability of Attack (P_a)

The annual probability is derived from a multi-year cumulative probability estimate using the actuarial complementary survival function -- the standard transformation from a periodic probability to an annual rate.

Primary formula (Bernoulli process):

```
P_a = 1 - (1 - P)^(1/Y)
```

Preferred alternative (Poisson arrival model):

```
P_a = 1 - e^(-lambda) where lambda = expected attacks per year
```

Variable	Definition	Calibration Guidance
`P_a`	Annual probability of a cyber attack (0 < P_a < 1)	Calculated
`P`	Cumulative probability of at least one attack over Y years	MITRE ATT&CK frequency tables; insurer actuarial loss data
`Y`	Time horizon over which P is estimated (years; typically 3-5)	Analyst judgment
`lambda`	Expected attacks per year (Poisson rate) [preferred when available]	Threat intelligence feeds; insurance carrier data

Mathematical note: The Bernoulli formula is formally correct only when annual attacks are independent and identically distributed (i.i.d.). In cyber risk, persistent threat actors and correlated vulnerability windows violate i.i.d. The Poisson model is

mathematically preferable when lambda is available from threat intelligence sources.

Step 3 | Annualized Loss Expectancy (ALE)

The Annualized Loss Expectancy is the cornerstone of quantitative risk analysis and is identical to the ALE metric defined in NIST SP 800-30. It translates a single-event cost into an annual expected loss, enabling direct comparison with annual cybersecurity program costs.

Formula:

```
ALE = TC x P_a
```

Variable	Definition
`ALE`	Annualized Loss Expectancy ($) -- expected dollar loss per year from cyber attacks
`TC`	Total Cost of Cyber Attack (from Step 1)
`P_a`	Annual Probability of Attack (from Step 2)

ALE is a mean estimate. For log-normally distributed cyber losses (empirically well-supported), the 95th-percentile loss can be 5x-15x the mean. Supplement ALE with Value-at-Risk (VaR) and Conditional Value-at-Risk (CVaR) from Monte Carlo simulation for board and insurer reporting.

Step 4 | Annualized Cost of Cybersecurity Program (ACC)

The annualized program cost spreads total investment across its expected useful life, analogous to straight-line depreciation in accounting. For programs with significant upfront capital expenditure, an NPV-adjusted annualization is strongly preferred.

Standard formula (straight-line):

```
ACC = C_prog / N
```

NPV-adjusted formula (recommended when WACC is available):

```
ACC_NPV = C_prog x [r / (1 - (1+r)^(-N))]
```

Variable	Definition	Guidance
`ACC`	Annualized Cybersecurity Program Cost ($)	Calculated
`C_prog`	Total program cost over deployment lifetime: licensing, personnel, training, infrastructure, services	Include fully-loaded labor costs; all-in TCO
`N`	Expected program lifespan (years)	Typically 3-5 years; align with tech refresh cycle
`r`	Discount rate (WACC or hurdle rate) [for NPV-adjusted formula only]	Finance team WACC; typically 8-15% for enterprise

Step 5 | Gross Margin Impact (GMI) and ROI

The Gross Margin Impact measures the net financial benefit of deploying the cybersecurity program. A positive GMI indicates that expected annual loss avoidance exceeds the annualized program cost. The original formula implicitly assumed 100% effectiveness -- a critical flaw corrected here.

Corrected formula (with explicit effectiveness coefficient):

```
GMI = (ALE x Effectiveness) - ACC
```

Derived ROI metric:

```
ROI = GMI / ACC = (ALE x Effectiveness - ACC) / ACC
```

Variable	Definition	Range / Default
`GMI`	Gross Margin Impact ($); positive = net benefit	Calculated
`ALE`	Annualized Loss Expectancy (from Step 3)	From Step 3
`Effectiveness`	Program risk reduction coefficient: fraction of ALE eliminated by controls	0.0-1.0; empirically 0.30-0.85 (Cyentia 2022)
`ACC`	Annualized Cybersecurity Program Cost (from Step 4)	From Step 4
`ROI`	Return on Investment; industry benchmark for mature programs: 2x-7x	Calculated

CRITICAL: The original formula (GMI = ALE - ACC) assumed Effectiveness = 1.0, meaning 100% risk elimination. No deployed security program achieves this. Effectiveness must be explicitly set. Cyentia Institute (2022) empirical ranges: Tier 1 maturity = 0.30-0.45; Tier 3 = 0.60-0.75; Tier 5 = 0.80-0.85. Leaving Effectiveness implicit produces materially overstated GMI and ROI figures.

3. Algorithm Summary

Step	Output Metric	Formula	Key Inputs
1	Total Cost (TC)	`TC = C_d + C_i`	Direct costs (response, legal) Indirect costs (revenue loss, reputation)
2	Annual Probability (P_a)	`P_a = 1-(1-P)^(1/Y)` `or 1-e^(-lambda)`	Cumulative probability P, horizon Y or Poisson rate lambda
3	Annualized Loss Expectancy (ALE)	`ALE = TC x P_a`	TC from Step 1 P_a from Step 2
4	Annualized Program Cost (ACC)	`ACC = C_prog/N` `or NPV-adjusted`	Total program cost, lifespan N WACC rate r (for NPV formula)
5	Gross Margin Impact (GMI) & ROI	`GMI = ALE x Eff - ACC` `ROI = GMI / ACC`	Effectiveness coefficient (0-1) ALE, ACC

Table 1. RQE Five-Step Algorithm -- step, output metric, canonical formula, and required inputs.

4. Worked Numerical Example

The following scenario illustrates the algorithm end-to-end for a hypothetical mid-market financial services firm with $200M annual revenue.

Input Parameter	Value	Source / Notes
Direct Costs (C_d)	$1,200,000	IR retainer + legal + regulatory fines
Indirect Costs (C_i) -- 1.5x multiplier applied	$3,000,000	Revenue loss + churn + brand impact
Total Cost (TC)	$4,200,000	Step 1: C_d + C_i
Cumulative probability P (3-year horizon)	45%	Industry threat intelligence
Time horizon Y	3 years	Analyst estimate
Annual Probability P_a	17.4%	Step 2: 1-(1-0.45)^(1/3)
Annualized Loss Expectancy (ALE)	$730,800	Step 3: $4.2M x 0.174
Total Program Cost (C_prog)	$1,500,000	3-year vendor contract
Program Lifespan (N)	3 years	Contract term
Annualized Program Cost (ACC)	$500,000	Step 4: $1.5M / 3
Effectiveness Coefficient	**0.70 (70%)**	**Tier 3 security maturity (Cyentia)**
Gross Margin Impact (GMI)	**$11,560**	**Step 5: $730.8K x 0.70 - $500K**
ROI	**2.3%**	**$11,560 / $500,000**

Table 2. Worked example -- hypothetical $200M financial services firm. Green rows indicate final computed outputs. Effectiveness of 0.70 reflects Tier 3 security program maturity.

Interpretation: At 70% effectiveness and a 17.4% annual attack probability, the investment produces a positive but modest GMI of approximately $11,560 annually. Increasing effectiveness to 0.80 (Tier 4 maturity) produces GMI of $84,640 -- an 8x improvement. This sensitivity illustrates why effectiveness parameterization is the most consequential input in the model and why security maturity investment produces non-linear financial returns.

5. Model Limitations and Recommended Extensions

Single-event assumption. The model calculates cost for a single attack type. Organizations facing multiple independent threat vectors (ransomware, data breach, DDoS, insider threat) should sum ALE across all threat categories rather than using a single composite TC value.

Point estimate vs. loss distribution. ALE is a mean. Boards and CFOs increasingly require tail-risk metrics. Supplement ALE with 90th and 95th percentile loss figures from Monte Carlo simulation. RQE's Exposure Modeling module provides these directly via the API.

Static annual probability. P_a is treated as constant across years. Threat landscapes evolve. RQE recommends annual recalibration using updated threat intelligence feeds and insurer actuarial tables. A time-varying P_a(t) model is preferable for multi-year planning horizons.

Effectiveness treated as constant. Controls degrade over time absent continuous investment. Effectiveness should be modeled as a decreasing function of program age, consistent with NIST CSF maturity degradation literature. RQE's Remediation Tracking module monitors actual effectiveness over time.

Correlation and systemic risk. In correlated threat environments such as supply chain attacks, individual firm ALE understates systemic exposure. Portfolio-level cyber risk models are required for enterprise conglomerates and organizations with heavy third-party dependencies.

Omitted option value. A complete analysis should include the option value of avoided regulatory sanctions, M&A; due diligence discounts, and cyber insurance premium reductions -- all of which produce GMI benefits not captured in the base model and frequently exceed the direct ALE avoidance benefit.

6. RQE API Integration

The Binary³ RQE API exposes each of the five algorithm steps programmatically through a RESTful JSON interface. Security platforms, SIEMs, SOAR tools, and GRC dashboards can embed real-time risk scoring by posting asset and threat context to the endpoint and receiving structured financial impact outputs in return.

RQE API Module	Algorithm Step	Output
Core Scoring	Steps 1-5	ALE, ACC, GMI, ROI as structured JSON
Exposure Modeling	Step 3 extension	Loss distribution: mean, P90, P95, CVaR
Assumption Detection	All steps	AI-flagged input assumptions and confidence gaps
Cost-Benefit Analysis	Step 5 extension	ROI curves and effectiveness sensitivity table
Remediation Tracking	Steps 4 & 5	Risk reduction over time as program matures

RQE API Module	Algorithm Step	Output
Historical Trend	Step 2 extension	P_a trend line and anomaly detection

Table 3. RQE API modules and correspondence to the five-step algorithm.

7. Conclusion

The Binary³ RQE financial methodology provides a commercially viable and mathematically defensible framework for translating cybersecurity risk into dollar terms accessible to CFOs, boards, and insurers. By grounding the model in actuarial expected loss theory, aligning with the FAIR ontology and NIST SP 800-30, and exposing the full algorithm through an API-first architecture, RQE enables organizations to make data-driven cybersecurity investment decisions with quantified confidence.

The five improvements introduced in this version -- explicit effectiveness parameterization, Poisson model alternative, NPV discounting, tail-risk supplementation, and multi-vector summation -- bring the model to institutional-grade standard suitable for insurance underwriting, M&A due diligence, and regulatory capital allocation.

References

• IBM Security / Ponemon Institute (2023). Cost of a Data Breach Report. IBM Corporation.

• Verizon (2024). Data Breach Investigations Report (DBIR). Verizon Business.

• The Open Group (2020). FAIR Model Standard C20B: Factor Analysis of Information Risk.

• NIST (2012). SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. NIST.

• Cyentia Institute (2022). Information Risk Insights Study (IRIS). Cyentia.

• MITRE Corporation. ATT&CK; Framework: Threat Frequency and Prevalence Data.

• Gartner (2023). Market Guide for IT Risk Management. Gartner Research.

• Binary³ (2025). RQE API Documentation and Research Methodology. binarycubed.com/rqe