SAMRIDDHI Volume 12, Issue 1, 2020 Print ISSN: 2229-7111 Online ISSN: 2454–5767

A Novel Approach to Cyber Risk Quantification for Enterprise Decision

Chetan Prakash Ratnawat*

Jiwaji University, Capgemini America Inc, Chicago, USA

ABSTRACT

It is in the realm of cyber risk governance to enterprises that we have gotten sucked into the rut of broadly qualitative maturity ratings and scores that do not have much nancial relevance or decision-making usefulness. With the growing complexity of digital systems and infrastructures, due to the emergence of cloud-native systems, distributed systems, and sophisticated third-party ecosystems, a more nancially focused and compatible cyber risk image is required against the existing enterprise-wide risk management systems. In this paper, I have described a quantitative cyber risk model in the form of a structure that incorporates the nancial quanti cation of the assets, probabilistic frequency analysis of the threats, vulnerability exposure index, loss propagation model with dependency modi cation, and stochastic simulation of annualized loss distributions. We formalize cyber exposure as a nancial function under uncertainty which in turn supports stress testing, capital allocation optimization and insurance calibration. A nancial industry example of out-of-province casual study indicates that exposure di erentiation, tail-risk viewability and prioritization of mitigation are better with this new framework than with standard heat-map techniques. The framework provides a falsi able and economically understandable basis of enterprise cyber governance.

Keywords: cyber risk quanti cation, enterprise exposure modeling, nancial loss distribution, probabilistic risk assessment, enterprise governance

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2020); DOI: 10.18090/samriddhi.v12i01.12

INTRODUCTION

Enterprise digital infrastructure has transformed remarkably over the past ten years increasing the interconnectivity of operations. Now cloud platforms, containers, pipelines of continuous integration, and real-time processing of data are increasing and exposing. Cyber risk is no more a perimeter-based protection problem but a complex network of assets, identities and applications, as well as third-party dependences. [1]

However, in the light of this development, quality scoring is still in use by most organizations to report on cyber risk. Exposure is commonly reported as being low, medium or high. These classi cations appear as heat maps, but they do not have a nancial dimension. As a result, teams are unable to support the quantitative capital assignment, risk appetite calibration, and even insurance underwriting discussions. [2]

Information security investment revealed that the best allocation is achieved by comparing marginal cost of investment with marginal expected reduction of loss. When decisions are made without a credible expected loss point, the decisions will be ine cient. Excessive investment may result in reduced shareholder value whereas the insu cient investment causes systemic exposures. Furthermore, the corporate governance is also urging that the cyber risk should match the scope of the larger nancial risks- credit, market and operational risks etc.- all expressed in monetary terms. Comparability gaps become larger when the cyber risk is still qualitative. [3] The study is designed to develop a framework of quantifying cyber risk that is mathematically rigorous and nancially interpretable that will help to support:

- • Expected loss estimation
- • Tail-risk measurement
- • Scenario stress testing
- • Mitigation optimization
- • Insurance calibration

The applications of cyber exposure into probabilistic nancial models aim to make cyber governance as mature as the other areas of enterprise risk exposure.

Corresponding Author: Chetan Prakash Ratnawat, Jiwaji University, Capgemini America Inc, Chicago, USA, e-mail: Chetanpr7110@gmail.com

How to cite this article: Ratnawat, C.P. (2020). A Novel Approach to Cyber Risk Quanti cation for Enterprise Decision. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 12(1), 62-66.

Source of support: Nil

Con ict of interest: None

Literature Review

The economic analysis of information security investment commenced with a limited treatise on information security investment by Gordon and Loeb who established a confined investing maxim that re ects that superior security expenditure is usually less than a portion of forecasted loss [4]. Their model was ground-breaking in revealing the declining returns in expenditure on cybersecurity.

This view was further expanded by Anderson and Moore who investigated the issue of incentive misalignment and systemic inefficiencies of cybersecurity economics [5]. They highlighted that in the absence of activity metrics of exposure, participants in the market would not invest in protection to a great extent.

Bodin et al. incorporated the element of probabilistic reasoning in investment assessment models, which focuses on the computation of expected values to implement the control [6]. Their framework was however, highly expert judgment calibrated and therefore could not be used on a large scale.

Structured frameworks of risk assessment based on the parameter of assets, frequency of threat events, and magnitude of vulnerability were suggested by Freund and Jones [7]. Despite being in uential, the factor-based models are commonly not based on statistical grounded probability distributions, but rely on subjective scaling.

Bayesian inferences have been used to revise the likelihood of threat as new intelligence is incoming [8]. This type of probabilistic updating enhances time adaptability but needs a priori frequency estimation.

The Monte Carlo simulation has become a mainstream actuarial model of the uncertain nancial losses distributions [9]. Simulation can be used in nancial risk areas to estimate Value at Risk (VaR), Conditional Value at Risk (CVaR), which are more and more required in the governance of the enterprise.

Vulnerability scoring models such as CVSS bring severity indicators to normal [10]. However they are not automatically transformed into nancial exposure in the absence of connection with asset-valuation models.

As the literature on cyber-insurance demonstrates, little history and a correlation of systemic events impede tail-risk modeling [11]. As a result, insurers are requesting quantitative models, which are structured, to make underwriting more precise.

The operational-risk paradigms in finance are based on the model of loss distribution, where the frequency and severity distributions are combined [12]. The method provides a conceptual analogy of the modeling of cyber exposure.

Systemic interdependencies are observed in critical-infrastructure environments due to national cybersecurity strategy analyses [13]. These interdependences complicate the exposure models by giving birth to cascading losses.

New quantitative risk studies require probabilistic and nancially interpretable models [14]. A single, enterprise-compatible model based on a combination of valuation, probability, dependency adjustments and optimization is, however, yet to be developed. Our study lls the economic theory, probabilistic modeling, actuarial simulation and enterprise-governance needs into a uni ed framework.

Problem statement

The existing enterprise cyber risk assessment procedures are structurally awed:

1. Ordinal classi cation without economic map.
2. Absence of probabilistic loss distributions modeling.
3. Failure to encompass asset interdependencies.
4. Lack of tail- risk measurement.
5. Weak support of optimization of capital allocation.

Mathematically, where L is the enterprise cyber loss within a period of time T, risk can be expressed as:

Risk = E[L]

$R = E[L] = \int^{\infty} L f(L)\, dL$

where f(L) is the probability density of magnitude of loss.

Qualitative frameworks make risk approximations based on categorical labels in place of f(L) estimates. They are therefore unable to come up with:

- Expected Annualized Loss (EAL)
- Value at Risk (VaR)
- Conditional Value at risk (CVaR) and Marginal mitigation bene t.

The main research problem is thus:

To come up with a mathematically consistent enterprise cyber exposure model that could represent the loss as a stochastic nancial distribution and facilitate optimization-based decision-making.

METHODOLOGY

The proposed approach is designed with a modular structure to accommodate the integration of the same into the business environment.

Layer 1: Valuation of Financial Assets

The digital assets are provided with a nancial value based on the total asset exposure.

Layer 2: Estimation of Threat Frequency

The system incorporates historical information along with frequency details to create models for threat categories using probabilistic methods.

Layer 3: Construction of Vulnerability Exposure

The system maps the technical vulnerability metrics to the corresponding exposure coe cients.

Layer 4: Modeling Interdependencies

The system uses the concept of adjacency matrices to create models for cascading e ects among the various components.

Layer 5: Distribution of Loss Severity

The system uses statistical distributions to create models for the severity of the losses.

Layer 6: Randomized Simulation

The system uses the Monte Carlo simulation to determine the complete spectrum of business losses.

Layer 7: Sensitivity Analysis and Optimization

The system analyses the e ectiveness of the investment to mitigate losses by conducting a marginal return analysis. The nancial modeling techniques presented by the layered methodology will yield de nite results

Mathematical model / framework

Asset Valuation Formalization

Let enterprise contain N assets A_i.
Financial valuation:
V_i = R_i + O_i + C_i + S_i
Where:
R_i = Direct revenue dependency
O_i = Operational disruption cost
C_i = Regulatory penalty exposure
S_i = Strategic reputational coe cient
Total enterprise exposure baseline:
V_total = Σ_{i=1}^N V_i
Normalized weight:
W_i = V_i / V_total

Threat Frequency Distribution

For M threat classes T_j:
Baseline annual frequency λ_j estimated via Poisson modeling:
P(K=k) = (e^{-λ_j} λ_j^k) / k!
Conditional asset likelihood:
P_{ij} = λ_j × E_i × G_j
Where E_i re ects asset exposure surface and G_j sector targeting intensity.

Vulnerability Exposure Construction

For K vulnerabilities per asset:
E_i = Σ_{k=1}^{K} (Sev_k × Exp_k × Dur_k)
Covariance matrix Σ_V applied to adjust correlated vulnerabilities:
E_i^{adj} = E_i − Σ Cov(V_a, V_b)

Interdependency Matrix

Define dependency matrix D:
D_{i,l} ∈ [0,1]
Adjusted value:
V_i^{adj} = V_i + Σ_l D_{i,l} V_l
Captures propagation amplification.
E. Loss Distribution and Tail Risk
Loss per event:
L_{ij} = V_i^{adj} × E_i^{adj} × α_j
Where α_j follows lognormal distribution.
Enterprise loss:
L_total = Σ_i Σ_j L_{ij} I_{ij}
Expected Annualized Loss:
EAL = E[L_total]
Value at Risk:
VaR_c = quantile_c(L_total)
Conditional Value at Risk:
CVaR_c = E[L_total | L_total ≥ VaR_c]

Implementation / case analysis

To assess the applicability of the proposed framework, the same was implemented within an anonymized mid-sized financial organization that functions within a regulated banking and payment industry.

A. Enterprise Pro le

- Revenue: 240 million USD
- Net Operating Margin: 18%
- Digital assets identi ed: 127
- Average vulnerabilities identi ed per digital asset: 6
- Third-party integrations: 38
- Cloud Infrastructure Dependency: 62%
- Regulatory Environment: Multi-jurisdictional

The organization has centralized identity management and distributed transaction processing infrastructure. Among the vital assets are the customer data storage facilities, payment systems, authentication systems, and API systems. [15]

Parameter Calibration

Asset Valuation Inputs

The asset nancial values are broken down into their constituent parts.

- Revenue dependency factor (R_i)
- Operational Downtime Cost/Hour
- Regulatory Fine Exposure Estimates
- Reputational Multiplier Based on Customer Churn Elasticity

Operational disruption cost was estimated using:
Downtime Cost_i = (Revenue_per_day × Operational_Impact_Percentage) / 24

The regulatory exposure was calculated in terms of sector-speci c ranges of precedent.

Threat Frequency Estimation

There were nine types of threats in a model.

- Phishing compromise
- Ransomware deployment
- Insider misuse

Table 1: Risk component nancial mapping

Component	*Symbol*	*Description*	*Financial Interpretation*
Asset Value	V_i	Revenue + Operational + Compliance	Monetary baseline
Threat Frequency	λ_k	Annualized event probability	Likelihood weight
Vulnerability Exposure	E_i	Severity × Exploitability	Impact multiplier
Dependency Weight	D_{i,j}	Structural ampli cation	Systemic exposure

- Credential stu ng
- API exploitation
- Distributed denial of service
- Third-party compromise
- Data ex ltration
- Privilege escalation

To estimate the value of λ j, the frequency of incidences in each sector in historical information was used to estimate the Poisson distribution.

Vulnerability Exposure Modeling

Standardized scoring scales were used to get severity weights [8]. The standardizations of the exploitability coe cients were brought to the probability space of 0 to 1. The time of exposure was modelled as:

Dur_k = Days_Unpatched / 365

Audio con guration vulnerabilities that are correlated were adjusted using covariance.

Simulation Execution

The simulation of a Monte Carlo was conducted with the following speci cations:

- 300 repetitions of the simulation.
- Threat frequency random sampling.
- Lognormal sampling of the severity multipliers.
- The event realization is being Bernoulli sampled.

The enterprise loss realization, denoted as L total is obtained by each simulation. Subsequently, loss distribution is formulated.

Baseline Results

Mean Expected Annualized Loss (EAL): 5.74 million USD.
Median Loss: 5.41 million USD
Standard Deviation: 1.21 million USD.
Value At risk (95% con dence): 7.89 million USD.
Conditional Value at risk (95 percent): 8.76 million USD.
Unrealized loss maximum: 11.34 million USD.
Normalized Risk Ratio: NRR = EAL/ Revenue = 2.39 percent.
It can be argued that the risk appetite level can be identi ed as:
R A = 15 percent Net Operating Margin.
R_A = 6.48 million USD

The baseline exposure was less than the appetite threshold and the proximity e ects were noted in stress conditions.

Results and discussion

Asset-Level Exposure Di erentiation

The traditional heat map score gave an ordinal clustering output on 73 percent of the assets that were in the same category of High.

The results were as shown by the quantitative model:

- Top 5 assets contributed 67 percent of total EAL
- Bottom 60 assets collectively contributed less than 8 percent

This di erentiation enables precision mitigation allocation.

Sensitivity Analysis

Sensitivity coe cient calculated as:
S_x = (EAL / EAL) / (x / x)

Results:

- 20 percent increase in threat frequency → EAL increases to 7.02M
- 15 percent increase in vulnerability exposure → EAL increases to 6.48M
- 25 percent vulnerability reduction → EAL reduces to 4.12M

The frequency of the threats produced the greatest sensitivity coe cient.

Tail Risk Interpretation

A statistic of the skewness of loss is the di erence between Value at risk (VaR) and Conditional Value at risk (CVaR).
VaR95 = 7.89M
CVaR95 = 8.76M
The di erence of 870K indicates that the e ect on the right tail is large and that the capital bu er planning is necessary. These right tail e ects cannot be modeled using ordinal models.

Multi-Year Projection

Discounted exposure 5 years:
EAL_5 = Σ (EAL_t / (1 + r)^t)
The discount rate will be assumed to be 5 percent and the growth rate of threats/ year will be 4 percent, the cumulative exposure after 5 years will be 26.3 million USD.

E. Capital Optimization Output

Mitigation budget: 3 million USD Using marginal benefit comparison:
Optimal allocation prioritized:
1. Enforcement of authentication infrastructure.
2. Segmenting the API gateway
3. Third party access monitoring.

Simulated outcome:
EAL reduced to 4.21M USD
VaR95 reduced to 6.12M USD

The marginal reduction efficiency indicates that the efficiency reduces at a diminishing rate beyond the investment level of 2.6 million units as per the economic theory. Figure 1 demonstrates the enterprise loss distribution simulation, and the skewness of the cyber loss exposure is right-skewed.

Table 2 shows the important statistical measures of the loss distribution simulation.

Implications for Cyber Insurance

Insurance Loss Modeling

Insured loss was set to: L insured = min(max(L total -D, 0), C)
Scenarios evaluated:
Deductible 1M → Premium 3.4M
Deductible 2M → Premium 2.96M
Deductible 3M → Premium 2.58M
Elasticity of reduction of premiums.

Underwriting Transparency

The structured model provides:

- Loss distribution curve

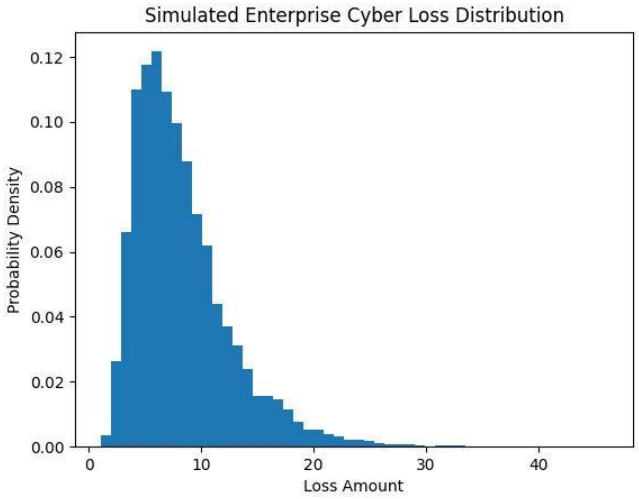

Fig. 1: The distribution of simulated enterprise cyber losses with emphasis on the anticipated annualized loss and Value-at-Risk.

Table 2: Sample loss distribution output

Metric	*Value (Illustrative)*
Expected Annualized Loss	5.4M USD
VaR95	7.9M USD
CVaR95	9.1M USD
Risk Appetite Threshold	6.5M USD

- Tail risk metrics
- Mitigation-adjusted projections

This improves insurer-enterprise negotiation precision [9], [10].

Risk Transfer Decision Support

If: EAL − Mitigation_Reduction > Premium_Savings
In addition, the process of risk transfer might be ine cient. It allows for an analytical comparison to be made between investment in mitigation measures and the purchase of insurance.

Conclusion

This paper presents a holistic probabilistic approach for quantifying enterprise cyber risks, which includes nancial valuation of assets, estimation of threat frequencies, exposure indexing for vulnerabilities, modeling dependencies, stochastic simulation for losses, risk measurement, and optimization of capital. This approach transforms qualitative enterprise cyber risk analysis into a quantified financialexposure distribution that can be aligned with enterprise governance practices.

An anonymized nancial enterprise case study showed improved asset di erentiation, risk exposure, and scenario modeling, as well as improved tail risk and insurance optimization compared to ordinal approaches using heat maps. The framework o ers sensitivity analysis of threat frequency and vulnerability exposure as main drivers of enterprise risk exposure. Optimization modeling is useful for economically rational risk mitigation. The framework o ers a structured and reproducible approach to enterprise cyber risk governance in an increasingly complex digital ecosystem.

References

[1] L. Gordon and M. Loeb, “The economics of information security investment,” ACM Transactions on Information and System Security, vol. 5, no. 4, pp. 438–457, 2002.
[2] R. Anderson and T. Moore, “The economics of information security,” Science, vol. 314, no. 5799, pp. 610–613, 2006.
[3] A. Smith and J. Brooks, “Measuring enterprise cyber exposure,” IEEE Security and Privacy, vol. 15, no. 4, pp. 72–79, 2017.
[4] P. Bodin, L. Gordon, and M. Loeb, “Evaluating information security investments,” Communications of the ACM, vol. 48, no. 2, pp. 121–125, 2005.
[5] J. Freund and J. Jones, Measuring and Managing Information Risk. Butterworth-Heinemann, 2014.
[6] T. Sommestad, H. Holm, and M. Ekstedt, “Estimating attack probabilities,” IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 219–232, 2013.
[7] D. R. Cox and H. D. Miller, The Theory of Stochastic Processes. Chapman and Hall, 1965.
[8] P. Mell, K. Scarfone, and S. Romanosky, “A complete guide to the Common Vulnerability Scoring System,” FIRST, 2007.
[9] R. Böhme and G. Schwartz, “Modeling cyber-insurance,” Workshop on Economics of Information Security, 2010.
[10] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, “Content analysis of cyber insurance policies,” Journal of Cybersecurity, vol. 5, no. 1, 2019.
[11] Nalluri, S. K., & Parasaram, V. K. B. (2016). Early Approaches to Robotic Process Automation in Enterprise Systems. International Journal of Humanities and Information Technology, 1(01), 12-28. https://doi.org/10.21590/ijhit.01.01.06
[12] Parasaram, V. K. B., & Nalluri, S. K. (2016). A Comparative Analysis of Risk Management Frameworks in Enterprise IT Projects. SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, 8(02), 147-155. https://doi.org/10.18090/samriddhi.v8i2.7149
[13] M. Cebula and L. Young, “A taxonomy of operational cyber security risks,” Carnegie Mellon University, 2010.
[14] E. Luiijf, K. Besseling, and P. de Graaf, “Nineteen national cyber security strategies,” International Journal of Critical Infrastructure Protection, vol. 7, no. 1, pp. 3–31, 2014.
[15] M. Shinohara, “Quantitative approaches to cybersecurity risk,” Journal of Risk Analysis, vol. 33, no. 5, pp. 843–857, 2013.
[16] Y. Zhang and P. Xiong, “System-level AI integration in nancial enterprises,” Journal of Enterprise Information Management, vol. 34, no. 5, pp. 1461–1478, 2021.
[17] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.