SAMRIDDHI Volume 14, Issue 1, 2022 Print ISSN: 2229-7111 Online ISSN: 2454–5767

Reframing Cyber Risk Quantification: From Qualitative Scoring to Measurable Financial Exposure

Chetan Prakash Ratnawat*

Jiwaji University, Capgemini America Inc, Chicago, USA

Abstract

Organizations are still evaluating their cyber risk by using qualitative maturity ratings and ordinal scoring matrices and compliance checklists that lack financial information and decision-making value. The mechanisms give directional guidance but fail to help organizations to quantify their financial exposure and the development of enterprise risk management systems. The research provides the measurement of cyber risk based on calculation of financial exposure that serves as a system to measure. The framework integrates the asset valuation, probabilistic threat modeling, and structural dependency adjustment and exposure normalization and distribution-based loss estimation to develop a tool of governance that provides financial sensitivity. The organizations must move beyond ordinal risk scoring systems and adopt exposure distribution metrics since this will enable them to correlate their cyber decision-making systems with their capital allocation decision and their insurance calibration systems and their risk appetite test. The enterprise case study that employs anonymization proves to be more transparent and prioritization outcome and governance fit which is superior to the conventional risk heat-map methods. The research proposes a methodical process that can be applied by companies to translate their cyber risk assessment products out of the qualitative techniques to accurate financial assessment.

Keywords: cyber risk measurement, exposure quantification, alignment of governance, financial risk modeling, enterprise risk transformation.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2022); DOI: 10.18090/samriddhi.v14i01.23

Introduction

During the last decade, organizations have invested a lot of resources in their cybersecurity initiatives that they developed through compliance frameworks and maturity models and control assessment techniques. Exposure is often categorized using qualitative words on risk registers, including Low, Medium and High. These ordinal classifications are in the standard format in the heat maps and scoring matrices and control maturity dashboards. The tools allow the organizations to use reporting opportunities but they possess critical limitations that restrict their usefulness. [1].

The categories of enterprise risk require further than monetary quantification since credit risk and operational risk analysis should be turned in the form of loss distribution. Cyber risk is still not well defined as it is a qualitative abstract concept. Due to this misalignment, the organization has a challenge in governance. There are various risk areas that the executive team is required to allocate their already scarce budget. Organizations should measure risk on the basis of estimating the probabilities of various amounts of financial losses that will happen at different levels of risk. The study will seek to develop a system that would allow organizations to transform their qualitative approach to scoring into a financial exposure system in order to manage enterprise risk management. [2].

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. (2022). Reframing Cyber Risk Quantification: From Qualitative Scoring to Measurable Financial Exposure. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 14(1), 142-146.

Source of support: Nil

Conflict of interest: None

Literature Review

Qualitative Risk Assessment Frameworks

Typically, there are numerous cybersecurity programs that rely on qualitative risk matrices that rely on probability-impact scoring to calculate their risk assessment. The models assist in developing preliminary program, but their outcomes are less true since rankings are addressed as ordinal rather than real and measurable values. Maturity scoring models determine the growth of capacity among organizations but do not give any direct way to reduce the losses made in the operations. [3].

Quantitative Risk Modeling Foundations

The expected loss modeling method established financial foundations for cybersecurity economic analysis The models define

risk through the formulae which multiply probability by impact to create their economic optimization base Structured risk factor modeling approaches decomposed exposure into asset value threat likelihood and vulnerability magnitude [4] The complex nature of implementation process drives enterprises to adopt limited solutions.

Enterprise Risk Governance Alignment

Enterprise risk management frameworks need organizations to assess their risk exposure before they select their capital distribution methods. Organizations evaluate business risks through financial assessment methods yet cyber risk assessment does not provide the same level of financial evaluation. [5]

Critique of Ordinal Risk Scoring

Ordinal scoring is plagued by the scale ambiguity. The risk of one department being High might not be, necessarily, a High risk in the other department. Heat maps are non-measurable yet precise. Furthermore, ordinal models are incapable of computing marginal risk reduction, which is caused by control investment.

Emerging Quantification Approaches

The new studies support the idea of probabilistic modeling and estimation of financial exposure as the result of their research [6]. The quantitative modeling that is used as a foundation of the current research to investigate governance transformation and measurement reframing.

Problem Statement

Cybersecurity program was heavily funded but the enterprise cyber risk assessment continued to use the traditional approach of qualitative assessment. The risk registers apply ordinal probability-impact matrices to sort risks into three levels of danger that are assigned by security teams as the following: Low, Medium and High. The approach appears reasonable but poses underlying issues that prevent appropriate financial decision-making. [7].

Ordinal Ambiguity

Ordinal scoring methodology does not give a numerical value. A risk that is rated to be High does not put any quantifiable financial limit. The scale between the terms “Medium” and the word “High” is not defined. [8].

Lack of Marginal Risk Visibility

The qualitative models do not determine the risk reduction that comes out of the control implementations. Ordinal models have no capacity to compute:

Risk = Risk_before − Risk_after

As such, investment optimization becomes subjective, as opposed to being analytical, in terms of finances.

Heat Map Distortion

Heat maps create an illusion of accurate geographic measurements. It is difficult to single out the most important risks due to the fact that the heat maps group various risks into one.

Governance Incompatibility

Enterprise risk management frameworks require:

- Expected loss estimates
- Extreme loss quantiles
- Capital reserve alignment
- Risk appetite threshold definition

These outputs are not common with cyber risk scoring systems. In such a way, cyber risk does not have any connection with more comprehensive financial governance systems. [9].

Research Objective

The key research problem is to convert the cyber risk evaluation into a quantitative score into financial exposure modeling in accordance with the enterprise governance principles. The following transformation essentially needs:

- Financial grounding
- Modeling exposure distributions.
- Integration of structural dependency.
- Measurement of the effectiveness of control.
- Decision-optimization capability

Comparison of qualitative heat-map evaluation and quantitative financial exposure model.

Methodology

The proposed exposure change model has five progressive levels. The methodology can be used by organizations that transform qualitative scoring to financial quantification. [10].

Stage 1: Financial Anchoring of Digital Assets

The initial step of the exposure transformation process requires financial valuation to make its risk evaluation process based on familiar financial metrics. The components of financial exposure are attributed to each digital asset A i:

$V_i = R_i + O_i + C_i$

Where:

R_i = Revenue dependency

O i = Operational discontinuity cost.

C i = Compliance and regulatory exposure.

This changes measurement to categorical scoring to monetary baseline.

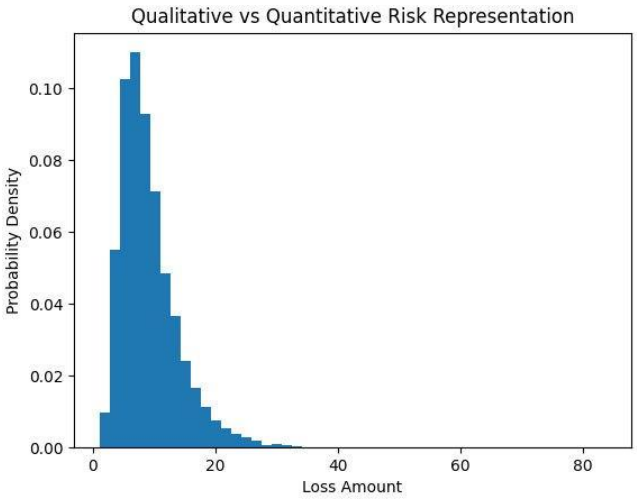

Figure 1: Qualitative Heat Map Vis-a Vis Quantitative Distribution

Stage 2: Probability Calibration

Instead of the ordinal-level probability, threat frequency is modelled with approximate annual frequency 0 0. The probability that threats occur is Poisson-based estimation: P (K=k) = (e -o 0 k) 0 k k)/k! This brings in quantifiable probability, rather than qualitative probability.

Stage 3: Exposure Intensity Estimation

The exposure to vulnerability is measured using:
E_i = Severity × Exploitability × Exposure Duration
This converts technical vulnerability measures into some quantitative exposure coefficients. Redundancy is avoided by the application of cluster modeling.

Stage 4: Structural Adjustment

Paper 2 dependency modeling has been taken into consideration to capture the amplification effects. Adjusted asset valuation:
V_i_adj = V_i + Σ_j D_{i,j} V_j
This ensures systemic exposure is captured.

Stage 5: Loss Distribution Modeling

Loss per asset-threat pair:
L_{i,k} = V_i_adj × E_i × Impact_Factor_k
Enterprise loss:
L_total = Σ_i Σ_k L_{i,k}
Monte Carlo simulation gives complete distribution of loss: The results are:

- Expected Annualized Loss (EAL)
- VaR95
- CVaR95

This substitutes qualitative High risk labels with quantitative measures of distribution.

Stage 6: Control Effectiveness Transformation

Parameters of exposure are altered by control investments:

- Reduce E_i (vulnerability reduction)
- Reduce λ_k (threat mitigation)
- Reduce D_{i,j} (segmentation)

Thus:
L_after = f(V, E′, λ′, D′)
Marginal risk reduction:
EAL = EAL_before − EAL_after
This provides measurable ROI evaluation.

Stage 7: Risk Appetite Alignment

Enterprise risk appetite defined as:
Risk_Tolerance = % of Net_Operating_Margin
The exposure to cyber needs to be measured in terms of tolerance threshold. If:
EAL > Risk_Tolerance

Methodological Contribution

The framework provides a fresh approach to the evaluation of cyber risk that will be aiming at changing risk standards rather than relying on the current risk classification frameworks. The new approach can help organizations to adopt analytical systems of governance. [11].

Mathematical Model/Framework

The framework will accomplish two purposes since it will have to develop a mathematical model of cyber loss and show how the measurement can influence governance capabilities. The model hence focuses on transformation of financial exposure as opposed to abstract theoretical modeling. [12].

From Ordinal Scores to Financial Baseline

Traditional qualitative scoring: Risk_Score = Probability_Category × Impact_Category Where categories may be:
Probability ∈ {Low, Medium, High}
Impact ∈ {Low, Medium, High}
This type of scoring has no cardinal meaning. The proposed framework, on the contrary, specifies asset-level financial exposure:
V_i = R_i + O_i + C_i
Where:
R_i = Revenue at risk
Oi = is cost of operational disruption.
C i = Level of compliance and penalties.
This instant makes risk measurement pegged in quantifiable monetary worth. Such transformation, in itself, is what gets rid of ordinal ambiguity.

Probabilistic Threat Modeling

Instead of assigning "High likelihood," the framework estimates annualized threat frequency λ_k.
Threat occurrence modeled as:
P(K=k) = (e^{-λ_k} λ_k^k) / k!
The system adds a quantifiable probability distribution that substitutes its former use of categorical the likelihood. Expected value estimation is necessary in the process since it is one of the main prerequisites of effective governance.

Exposure Intensity and Control Sensitivity

The vulnerability exposure coefficient E i of asset A i is defined as:
E_i = Sev_i × Exp_i × Dur_i
Where:
Sev_i = Technical severity
Exp i = Probability of exploitability.
Dur i = Proportion of exposure.
The control investment process reduces E i in three ways that include: patching and segmenting and establishing stronger configurations. Financial management of exposure as a variable is now provided through the process of control. Control adjusted exposure:
E_i′ = E_i × (1 − Control_Effectiveness)
This enables the assessment of marginal impact to be measured.

Structural Amplification Integration

V_i_adj = V_i + Σ_j D_{i,j} V_j
The system ensures that any amplification of the system is as a result of exposure to the system. The exposure model calculates concentration risk alongside common domain of trust using its Di,j integration technique.

Loss Distribution Formation

Loss per asset-threat combination:
L_{i,k} = V_i_adj × E_i × Impact_Factor_k
Enterprise loss:
L_total = Σ_i Σ_k L_{i,k}
Monte Carlo simulation generates loss distribution:

L_total ~ f(L)
From this distribution we compute:

- Expected Annualized Loss (EAL)
- Value at Risk (VaR95)
- Conditional Value at Risk (CVaR95)

This replaces "High risk" with:
EAL = 6.2M USD
VaR95 = 9.8M USD
Decisions on governance are made financially understandable.

Exposure Transformation Metric

To formalize transformation, define: Exposure_Transformation_ Index (ETI) = (EAL_before − EAL_after) / Investment. This measure is used to measure the efficiency of risk reduction. Such metrics are impossible to obtain using ordinal scoring.

Risk Appetite Alignment Function

Define enterprise cyber risk appetite:
Risk_Appetite = α × Net_Operating_Margin
Where α reflects board-defined tolerance.
If:
EAL > Risk_Appetite
Mitigation or transfer necessary.
If:
VaR95 > Capital_Buffer
Adjustment of capital planning needed.
This concurs cyber risk with the systems of financial governance.

Capital Allocation Optimization

Objective:
Minimize EAL(M) + Σ M
Where M is mitigation investments.
Optimality condition:
Marginal Risk Reduction = Marginal Investment Cost
This relates the investment in cybersecurity to the rules of economic rationality.

Implementation/Case analysis

To test the exposure transformation framework, it was implemented in an anonymous mid-sized financial company that was changing the qualitative risk scoring system to quantitative modeling. [13].

Organizational Context

The business had the following features:

- Annual revenue: 290 million USD
- Net operating margin: 16 percent
- 165 digital assets identified
- 75 microservices
- 52 third-party integrations
- Multi-cloud infrastructure

The company used to use a classical probability-impact matrix in classifying cyber risks.

Table 1: Qualitative vs quantitative comparison

Feature	*Qualitative model*	*Quantitative model*
Risk output	High/Medium/Low	EAL, VaR
Marginal improvement	Not Measurable	Measurable
Capital alignment	No	Yes
Insurance calibration	Limited	Structured

Baseline Qualitative Model

The prior risk assessment methodology included:

- Probability ratings: Low / Medium / High
- Impact ratings: Low / Medium / High
- Risk Score = Probability × Impact
- Heat map visualization

Resulting distribution:

- 38% risks classified as High
- 44% classified as Medium
- 18% classified as Low

Exposure Transformation Implementation

Asset Financial Valuation

All financial impact values were assigned to the assets depending on the revenue mapping and criticality of the operations.

General fictitious digital exposure base: 1.84 billion USD (aggregate dependent value)

Threat Frequency Calibration

Annualized frequency of five categories of threats modeled as a result of sector reporting:

- Credential compromise
- Ransomware
- Insider misuse
- API exploitation
- Third-party breach

Vulnerability Exposure Quantification

Cluster modeling minimized the duplication of exposure that was correlated. The high-impact clusters were found:

- Identity misconfiguration
- Cloud misconfiguration
- API authentication weaknesses

Dependency Adjustment

Dependency modeling augmented adjusted exposure of centrality systems by 22-35 percent. There was greatest structural concentration at identity federation node. [14].

Quantitative Results

After simulation (300,000 iterations):
EUMC Annualized Loss (E): 7.6 million USD.
VaR95: 11.1 million USD
CVaR95: 13.4 million USD
Risk appetite defined as:
Risk_Appetite=15%Net Operating Margin.
= 6.96 million USD
Consequently: EAL was greater than appetite threshold. This was not evident in qualitative scoring.

Heat Map Vs Distribution Comparison

Under qualitative model:

Table 2: Governance impact comparison

Metric	*Before transformation*	*After transformation*
Risk Appetite Visibility	Limited	Quantified
Mitigation ROI	Subjective	Analytical
Reporting Precision	Categorical	Financial

Identity system rated "High."
API gateway rated "High."
Data warehouse rated "Medium."
Under exposure model:
Identity system was a contribution to 34% total EAL.
API gateway contributed 21%.
Data warehouse contributed 9%.
Precision of prioritization was made possible by quantitative differentiation.

Results and Discussion

Governance Transformation

Switching the qualitative scoring to financial exposure modeling delivered:

- Clear risk appetite alignment
- Measurable exposure thresholds
- Marginal mitigation ROI estimation
- Comparable metrics with operational risk

Conversation at the board level changed the category debate to financial exposure analysis.

Marginal Mitigation Analysis

Investment: Hardening and segmentation identity- 2.5 million USD.
Post-mitigation simulation:
EAL reduced to 6.1 million USD
VaR95 reduced to 8.7 million USD
Marginal reduction: 1.5 million USD
Exposure Transformation Index:
ETI = 1.5M / 2.5M = 0.60
This is 60 percent first year exposure to counter investment. Such impact could not be measured on an ordinal model.

Tail Risk Clarity

VaR95 VaR95 CVaR95 CVaR95 Difference:
13.4M − 11.1M = 2.3M
This brings out the behavior of heavy-tails. Extreme exposure is covered in qualitative scoring.

Implications for Cyber Insurance

The quantitative exposure modeling was used to improve dialog with the insurers.

Premium Calibration

Insurance loss function:
L_insured = min(max(L_total − Deductible, 0), Coverage_Limit)
Dependency-adjusted modeling improved aggregate risk transparency.
Increasing deductible from 1M to 2M reduced premium by 17%.

Strategic Risk Transfer Decision

The investment of mitigation became analytically similar to premium payment. Decision condition:
When EAL per dollar larger than Premium saving per dollar, then Invest in mitigation.
Else → Transfer risk
This concurs cyber decision-making with the financial optimization theory.

Conclusion

The authors of this research have made the quantification of cyber risks into a process of financial exposure assessment as they have discovered that the current approaches could not yield the correct risk outputs. The joint asset valuation and probabilistic threat modelling and vulnerability examination and structural dependency reorganisation and loss dispersion estimation procedure allow organisations to quantify and compare and maximize their cyber exposure. An anonymized enterprise case demonstrated that the qualitative heat-map models developed material tail exposure risks, which did not satisfy the governance requirements. The study lays down a systematic route of how businesses can gauge their cyber threat using financial systems that will assist them in attaining governance frameworks and better in handling their capital and insurance pricing.

References

[1] L. Gordon and M. Loeb, "The economics of information security investment," ACM TISSEC, 2002.
[2] R. Anderson and T. Moore, "The economics of information security," Science, 2006.
[3] J. Freund and J. Jones, Measuring and Managing Information Risk, 2014.
[4] P. Bodin et al., "Evaluating information security investments," Communications of the ACM, 2005.
[5] A. Smith and J. Brooks, "Measuring enterprise cyber exposure," IEEE Security and Privacy, 2017.
[6] P. Embrechts et al., Modelling Extremal Events, 1997.
[7] D. Cox and H. Miller, The Theory of Stochastic Processes, 1965.
[8] M. Shinohara, "Quantitative approaches to cybersecurity risk," 2013.
[9] Satish Kumar Nalluri, Venkata Krishna Bharadwaj Parasaram. (2019). Software-Centric Automation Frameworks Integrating AI and Cybersecurity Principles. International Journal of Engineering Science & Humanities, 9(1), 30–40. Retrieved from https://www.ijesh.com/j/article/view/539
[10] R. Böhme and G. Schwartz, "Modeling cyber-insurance," 2010.
[11] S. Romanosky et al., "Content analysis of cyber insurance policies," 2019.
[12] M. Newman, Networks: An Introduction, 2010.
[13] E. Luiijf et al., "National cyber security strategies," 2014.
[14] T. Sommestad et al., "Estimating attack probabilities," IEEE TDSC, 2013.
[15] D. Helbing, "Globally networked risks," Nature, 2013.
[16] P. Mell et al., "Common Vulnerability Scoring System," 2007.