SAMRIDDHI Volume 13, Issue 1, 2021 Print ISSN: 2229-7111 Online ISSN: 2454–5767

Foundational Methods for Cyber Risk Quantification in Complex Digital Environments

Chetan Prakash Ratnawat*

Jiwaji University, Capgemini America Inc, Chicago, USA

Abstract

The digital environment of the business world is marked by digital ecosystems, which exhibit structural interdependencies, therefore, imposing an impact on the cyber exposure profile. Distributed systems, microservices systems, federated identity systems, and third-party systems result in tightly coupled systems where a nonlinear behavior of cyber compromise events occurs. The systemic risks of cyber exposure are likely to be significantly underestimated through the traditional methods of quantifying cyber risks that are usually linear aggregation of losses incurred by independent assets. The research formulates a quantitative model of cyber risk measurement that takes into consideration the challenges of digital ecosystems. This framework combines digital asset graph modeling, dependency weight estimation, threat vector stratification, vulnerability cluster evaluation, propagation-weighted financial loss calculation, and stochastic simulation. This framework embeds the effects of structural interdependencies into probabilistic modeling, which characterizes cyber exposure as a financially weighted, dynamically influenced distribution. An anonymized financial enterprise case demonstrates the benefits of the framework, which displays increased expected and tail losses with the inclusion of structural dependencies. This framework presents a foundational model for cyber risk quantification that can be scaled for financial evaluation for enterprise cyber governance.

Keywords: Cyber risk quantification, Complex digital systems, Systemic exposure, Graph-based modeling, Enterprise risk management

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2021); DOI: 10.18090/samriddhi.v13i01.12

Introduction

The development and growth of enterprise digital infrastructure fundamentally change the structural properties of cyber risk exposure. Conventional information systems are centralized with well-defined boundaries and isolated application stacks. In contrast, the digital infrastructure of the enterprise world has become distributed computing, microservices orchestration, identity federation, cloud service integration, and dynamic third-party connectivity. This has, in turn, resulted in digital infrastructure that does not behave in accordance with traditional system behavior; it is more of a network. [1]

In networked systems, the risk exposure is not just the inherent risk of the asset but is further compounded by the position of the asset in the network. Therefore, quantification of cyber risk, which is based on the asset as an independent entity, does not account for the "amplification effect." The enterprise boards and risk committees require an equivalent representation of cyber risk, as is the case with financial risk. In traditional enterprise risk management domains, including credit risk, market risk, and operational risk, the distribution of risk is based on correlation and the impact of systemic interactions. Therefore, quantification of cyber risk must be equivalent to account for these effects. [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. (2021). Foundational Methods for Cyber Risk Quantification in Complex Digital Environments. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 13(1), 65-70.

Source of support: Nil

Conflict of interest: None

The modern digital ecosystem is marked by five distinct attributes:

- The digital asset depends on shared services which include identity management and network infrastructure and database clusters.
- The application uses an architectural design which contains multiple layers of interdependencies because the application requires middleware and middleware needs infrastructure services to operate.
- The shared trusted domains experience system access because authentication systems face security breaches.
- Third-party service providers face risks because their operations depend on each other.
- Cloud-native applications are able to do dynamic reconfiguration.

© The Author(s). 2021 Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and non-commercial reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The Creative Commons Public Domain Dedication waiver (http://creativecommons.org/publicdomain/zero/1.0/) applies to the data made available in this article, unless otherwise stated.

The mixture of these features leads to random patterns of exposure. The failure of the central authentication service causes a chain reaction on all the applications whose service relies on it. In case of misconfiguration of the cloud environment, it leads to security issues, particularly since most of the services use shared infrastructure components. Enterprise cyber risk models are numerous and still use linear segregation of assets, even though the realities mentioned above exist. The following formula is used to calculate Expected Loss:

Expected Loss = Probability * Impact [3]

The procedure of determining the asset value is done without the aspect of relating the assets. Such an approach gives a true estimate to loosely coupled systems among the components. The research article outlines the crucial techniques that enable organizations to evaluate the cyber risk through modeling the interdependency as well as financial interpretability and applicability. [4].

Literature Review

Economic Models of Cyber Risk

The initial studies, which utilized economic models of investment in cybersecurity, established risk as an assessment of expected loss. Gordon and Loeb showed that an organization should align its optimal investment in cybersecurity with its current security weaknesses. Anderson and Moore showed that economic waste is present in the cybersecurity market, as it offers misaligned incentives in the current system. This shows the need for measurable exposure for rational decision-making. [5]

Structured Risk Quantification Frameworks

The development of the "structured quantification" approach enabled the systematic decomposition of risk into asset value, threat frequency, and vulnerability magnitude. Freund and Jones developed the risk factor modeling approach based on asset valuation, threat event frequency, and control effectiveness adjustment. Though the methodology was sound, the effects of interdependency were not captured. [6]

Dependency and Correlation Modeling

In financial operational risk modeling, the dependency between the risk factors is taken into account using correlation matrices and copula functions. These approaches prove the fact that the dependency between the risk factors should not be ignored, as this leads to the underestimation of extreme losses. Research conducted using the field of network science proved that the systems which are interconnected suffer from cascade failure when the key nodes are compromised. [7]

Vulnerability Correlation and Cluster Modeling

Vulnerability scoring systems, like CVSS, have standardized the measurement of severity. However, the existence of correlated vulnerabilities across shared platforms necessitates the use of cluster-based modeling to avoid redundant exposure estimation. Cluster modeling reduces the risk of overestimation by considering vulnerabilities with shared exploit pathways. [8]

Cyber Insurance and Aggregation Risk

Systemic aggregation risk is being discussed more within cyber insurance literature, especially for those organizations that share common cloud service providers or third-party infrastructures [9]. Insurers are struggling to effectively model catastrophic cyber events that are correlated. The aggregation risk emphasizes the need for structural dependency modeling within quantification schemes for the enterprise.

Problem Statement

The quantification of the risk of cyber-attacks in a complex digital ecosystem has certain structural and methodological issues, which are not adequately captured by existing risk assessment frameworks. Most of the existing risk models of cyber-attacks in the context of the enterprise world are based on certain assumptions of explicit or implicit independence of the digital assets. [10]

Structural Interdependency in Digital Systems

Let the enterprise digital environment be represented as a set of assets:

$A = \{A_1, A_2, \ldots, A_n\}$

In traditional independent-asset modeling, enterprise loss is expressed as:

$L\_total = \Sigma\_i\ L\_i$

Where L_i represents direct financial loss associated with asset A_i. However, in complex digital ecosystems, assets exhibit dependency relationships. For example:

- Application servers depend on identity services.
- Microservices depend on shared data stores.
- Internal systems depend on third-party authentication providers.
- Cloud-hosted workloads depend on shared infrastructure configurations.

Therefore, compromise in one asset may induce conditional exposure in another. To represent this formally, we define a dependency function:

$Dep(A\_i, A\_j) \rightarrow w\_\{i,j\}$

Where $w\_\{i,j\} \in [0,1]$ represents degree of reliance of asset A_i on asset A_j.

Under structural dependency, enterprise loss must incorporate propagation effects:

$L\_total = \Sigma\_i\ L\_i + \Sigma\_i\ \Sigma\_j\ w\_\{i,j\}\ L\_j$

This demonstrates that enterprise loss becomes topology-dependent rather than purely additive.

Non-Linearity of Exposure

The level of risk exposure in a highly integrated system has a tendency to increase over time, driven by the nature of a highly integrated system architecture. This results in a cluster effect, increasing the likelihood of extreme risk events. [11]

Tail-Risk Underestimation

If dependence is not taken into account, the expected loss (EAL) is underestimated because extreme loss quantiles, Value at Risk, and Conditional Value at Risk are subject to considerable underestimation. Risk measurement in the tail is a critical component of enterprise governance and alignment with insurance objectives.

Practical Modeling Challenge

In the absence of consideration of dependency, the expected loss (EAL) is underestimated because of the large underestimation of extreme loss quantiles (Value at Risk and Conditional Value at Risk).

Tail risk evaluation plays a vital role in enterprise governance and the alignment of insurance practices.

Methodology

In order to address the defined problem, the team presents a five-layer modeling framework, which allows for the implementation of the proposed solution by enterprises. The methodology supports the development of rigorous mathematical standards, as well as user-friendly operability.

Layer 1: Digital Asset Mapping and Classification

This involves a thorough asset identification, which is to be carried out before classification, in order to classify the assets into various classes or categories.

- Core Business Systems
- Identity and Access Management Infrastructure
- Data Repositories
- Application Service Layers
- Integration Gateways
- Third-Party Service Dependencies

A set of financial exposure parameters is assigned to each asset. [13]

- Revenue dependency coefficient
- Operational disruption impact
- Regulatory penalty multiplier
- Strategic reputational sensitivity

It may help simplify financial modeling before moving on to structural modeling.

Layer 2: Dependency Modeling Framework

- Identify whether A_i requires A_j for operation.
- Assign dependency weight w_{i,j}.

Dependency weights may be calibrated using:

- Service dependency documentation
- Architectural diagrams
- Operational workflow analysis
- Incident impact analysis

The weights are normalized to the interval [0,1] for interpretability. Therefore, a dependency matrix D of size n x n can be obtained.

Layer 3: Threat Vector Stratification

The threat modeling process involves a variety of analysis levels to identify various enemies' combatants. The system identifies three different threat categories, including various threats.

- Opportunistic external attacks (e.g., phishing, scanning)
- Targeted adversarial campaigns
- Insider misuse
- Supply chain compromise
- Credential abuse

Each threat class is assigned baseline annual frequency λ_j derived from historical incident data and sector analysis [12].

Layer 4: Vulnerability Cluster Modeling

Weaknesses in the digital ecosystem are frequently correlated. For example:

- Multiple services may share identical misconfiguration.
- Shared libraries may introduce common exploit paths.
- Misconfiguration of identity can provide a variety of services at the same time.

Layer 5: Propagation-Adjusted Loss Estimation

Direct loss for asset A_i under threat T_j:
$L_{direct}(i,j) = V_i \times E_i \times Impact\_Factor_j$
Propagation-adjusted value:
$V_{i\_adj} = V_i + \Sigma_j w_{i,j} V_j$
Adjusted loss:
$L_{adj}(i,j) = V_{i\_adj} \times E_i \times Impact\_Factor_j$
Enterprise total loss:
$L_{total} = \Sigma_i \Sigma_j L_{adj}(i,j)$
Expected Annualized Loss (EAL) computed through probabilistic simulation.

Layer 6: Simulation and Scenario Modeling

1. Sample threat events.
2. Sample impact multipliers.
3. The company employs propagation-based value of assets evaluation.
4. The organization calculates enterprise losses in total.

Simulation outputs:

Layer 7: Sensitivity and Structural Impact Analysis

The sensitivity analysis is undertaken on:

- Dependency weights
- Threat frequency
- Vulnerability cluster exposure
- Central node concentration

This determines the structural factors that impact on exposure to the greatest extent.

Methodological Advantages

This is a systematic method which gives:

- Financial interpretability
- Structural awareness
- Reduced overestimation through clustering
- Tail-risk visibility
- Enterprise implement ability

Mathematical Model/framework

The study is expected to employ monetary methods in quantifying the danger of cyber exposure in complicated computer networks, rather than merely theorize. The model is constructed progressively whereby the possibility of direct revealed assets to result in enterprise loss such as the dispersion of risk starts. [14].

Financial Valuation of Digital Assets

Suppose that the enterprise has N digital assets: A = {A1, A 2, A n). The financial valuation V i of each asset is broken down into three major parts: V i = R i + O i + C i.
Where:
Ri is Direct revenue dependency due to asset Ai.
O i = Operational disruption cost (downtime impact)
C i = Regulatory, legal, compliance exposure.
The cost of operational disruption is determined based on the service criticality and revenue impact ratios:

O_i = (Daily_Revenue × Impact_Percentage × Downtime_Hours) / 24

Structural Dependency Adjustment

Assets are not autonomous in complicated digital spaces. We construct a dependency matrix D with the following characteristics: D i, j [0,1] D i, j is the extent to which asset A i is operationally dependent on asset A j.

When A i is completely dependent on A j, D i, j tends to be equal to 1. In the event of non-existent relationship, D ij = 0.

Adjusted asset valuation:

V_i_adj = V_i + Σ_j (D_{i,j} × V_j)

The statement goes further to show that the more the asset that has to be verified fails, the higher the levels of exposure. The exposure of an authentication server that has five systems attached to it will increase when the attacker targets the authentication server. The interconnections between digital assets create ways through which there is magnifying effect as seen in Figure 1.

Threat Frequency Modeling

History of incidences in the sector is used to estimate the frequency λ T k of each category of threat T k. Threat occurrence is Poisson distributed:

P(K = k events) = (e^{-λ_k} λ_k^k) / k!

The categories of threats could be:

- Phishing-based credential compromise
- Ransomware deployment
- Insider data exfiltration
- API exploitation

Each threat category is modelled separately to preserve heterogeneity in likelihood and impact.

D. Vulnerability Cluster Modeling

Correlated weaknesses are clustered together in the Cm in place of assessing the vulnerabilities separately. Cluster exposure score:

E_m = Severity_m × Exploitability_m × Exposure_Duration_m

Where: Severity m- is a measure of magnitude of impact. Technical feasibility is represented by exploitability.

Exposure of Time: Exposure Length m indicates time unmitigated.

Cluster level modeling eliminates overlapping risk amplification of a service with misconfigurations in a shared fashion. For asset A_i, total exposure

E_i = Σ_m E_m

Propagation-Adjusted Loss Function

Direct loss of asset A i threatened by T k:

L direct (i,k) = V i adj x E i x Impact Multiplier k.

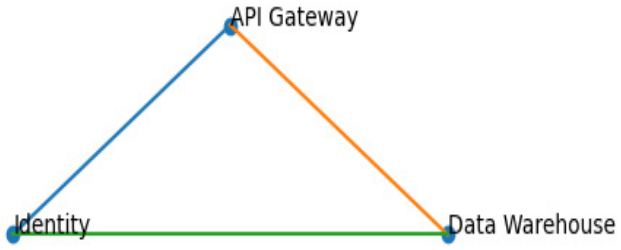

Fig. 1: Enterprise dependency graph of digital assets with pathways of structural amplification

Enterprise total loss:

L_total = Σ_i Σ_k L_direct(i,k)

L total since V iaj already has the dependency amplification effect, it is possible to reflect structural propagation effects without the complicated iterative matrix operations. This does not lose enterprise interpretability and still has structural realism.

Tail-Risk Quantification

Expected Annualized Loss:

EAL = E[L_total]

At confidence level c, Value at risk is:

VaRc = minimum value of such that

P(L_total ≤ VaR_c) ≥ c

Conditional Value at Risk:

CVaR opposed = loss expected to be below VaR threshold.

CVaR gives the information on the severity of catastrophic yet plausible events.

There is no structural amplification, making independent-asset models not much better at estimating VaR and CVaR.

Structural Concentration Risk

To measure structural concentration, centrality metrics are computed:

- Degree centrality: number of direct dependencies
- Weighted centrality: sum of dependency weights
- Dependency exposure index: Σ_j D_{i,j}

The nodes in the system are the assets whose values of dependency index are significant. The failure of these nodes can affect other nodes in the system, so the protection is done on these nodes. It has now a new component within the system that is not limited to the basic vulnerability assessment.

Multi-Period Exposure Projection

The exposure must be projected in horizons that span several years since digital environments change with time. Exposure projection in five years to come:

Table 1: Dependency Matrix Example

Asset	*Identity*	*API gateway*	*Data warehouse*
Identity	1.0	0.4	0.3
API Gateway	0.5	1.0	0.6
Data Warehouse	0.2	0.3	1.0

Table 2: Exposure before and after dependency adjustment

Metric	*Independent model*	*Dependency model*
EAL	5.4M	7.1M
VaR95	7.9M	10.2M
CVaR95	9.1M	11.8M

EAL_5 = Σ_{t=1}^{5} EAL_t / (1 + r)^t
Where:
r = discount rate
EALt takes into consideration the predicted rate of threat growth g.
Threat growth modelling: λ k(t) = λ k (0) × (1 + g)t.
This assists in alignment of strategic planning.

Model Interpretation

This incorporating system is effective in reaching:

- Financial grounding
- Structural realism
- Practical implement ability
- Governance compatibility

It does not have unduly abstract spectral derivations of the radius and maintains the systemic modeling fidelity.

Implementation/Case analysis

To conclude on the practical applicability of the framework, the proposed framework has been applied in an anonymized middle-size financial organization that is subject to regulatory authority by a number of jurisdictions.

Enterprise Structural Profile

The following characteristics were witnessed in the organization:

- Annual revenue: 275 million USD
- Net operating margin: 17 percent
- Total digital assets identified: 158
- Microservices deployed: 72
- Third-party API integrations: 48

There was an average high level of interdependence of the digital system between its components. The identity layer and the integration layer were connected, specifically.

Asset Financial Calibration

- Direct revenue dependency
- Operational downtime cost
- Compliance and regulatory exposure.

The dependence on the revenues was calculated with the help of mapping the digital assets and the generating workflow revenue. Determination of the cost of downtime was calculated as follows: Downtime_Cost = (Average_Daily_Revenue * Operational_Impact_Ratio) / 24

Dependency Mapping Results

- Identity federation service supported 41 dependent assets.
- API gateway connected 33 downstream services.
- Data warehouse served 27 analytics services.

Threat and Vulnerability Calibration

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

The sector incident reporting formed the basis of baseline annual frequency estimates. Vulnerabilities were categorised into a cluster such as:

- Identity misconfiguration cluster
- Shared library exposure cluster
- Cloud misconfiguration cluster
- API authentication weakness cluster

Cluster modeling reduced double-counting of correlated exposure.

Simulation Execution

Monte Carlo simulation was executed with:

- 250,000 iterations
- Randomized threat occurrence sampling
- Lognormal impact multiplier distributions
- Propagation-adjusted asset values

Each iteration produced enterprise loss realization Total. The resulting distribution exhibited right-skewed behavior typical of cyber loss.

Results and Discussion

Baseline Independent Model

Independent-asset modeling (without dependency adjustment) produced:

- Expected Annualized Loss (EAL): 5.4 million USD
- VaR95: 7.9 million USD
- CVaR95: 9.1 million USD

This model treated each asset as isolated.

Dependency-Adjusted Model

After structural propagation adjustment:

- EAL: 7.1 million USD
- VaR95: 10.2 million USD
- CVaR95: 11.8 million USD

The structural amplification increased the exposure by around 31.5%. "The tail risk increased more than the average loss. This underlines the concentration effect. Dependency-adjusted modeling shifts the loss distribution to the right, as shown in Figure 2."

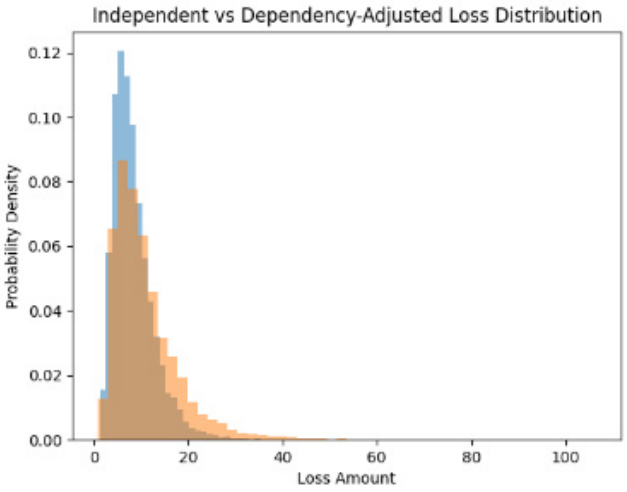

Fig. 2: Comparison of independent and dependency-adjusted loss distributions showing systemic amplification

Structural Amplification Interpretation

This increase in VaR far surpassed the increase in EAL, demonstrating that modeling dependencies largely affects the most severe events of loss. The nodes that had a high level of centrality contributed a disproportionate amount of risk. When identity infrastructures are breached, a large number of services are exposed at once. This is why the increase in risk was so large.

Sensitivity Analysis

Sensitivity coefficients were computed for key parameters:

- 10% increase in dependency weights → EAL increased by 8.2%
- 15% reduction in vulnerability cluster exposure → EAL reduced by 12.6%
- 20% increase in threat frequency → EAL increased by 18.4%

Mitigation Prioritization Impact

Mitigation focused on:

- Identity service hardening
- API gateway segmentation
- Multi-factor authentication enforcement

Simulation of targeted mitigation produced:

- EAL reduction to 5.9 million USD
- VaR95 reduction to 8.4 million USD

Implications for Cyber Insurance

Aggregation Risk Modeling

Propagation-adjusted models can produce realistic aggregate loss estimates when there is a correlation between the compromise scenarios. Independent models tend to underestimate catastrophe exposures for enterprises with high cloud concentration.

Deductible and Coverage Calibration

Insurance loss function:

L_insured = min(max(L_total – Deductible, 0), Coverage_Limit)

This has resulted in better premium calibration. When the deductible increased from $1 million to $2 million, the premium fell by 14 percent with the propagation-aware modeling.

Capital Allocation Decision Support

Enterprise must decide between:

- Additional mitigation investment
- Increased insurance transfer

Propagation-adjusted modeling enables us to analytically compare the additional benefit of mitigation to its premium cost. In other words, this approach brings cyber risk management into line with the principles of financial capital allocation [15].

Conclusion

This paper describes the essential approaches for quantifying cyber risk within complex digital systems. The approaches are a combination of digital asset mapping, dependency modeling, threat tiering, clustering of vulnerabilities, estimation of losses based on how breaches spread through a digital environment, and stochastic simulation. The results indicate that the dependencies between digital components significantly increase the expected risk value as well as the probabilities of large losses compared to approaches that assume digital assets are independent of each other. This risk increases significantly for digital assets located at the center of services such as identity services or integration gateways. This research offers the fundamental machinery towards the additional research on dynamic methods to evaluate the cyber risk.

References

[1] L. Gordon and M. Loeb, "The economics of information security investment," ACM Transactions on Information and System Security, 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] M. Newman, Networks: An Introduction, 2010.
[7] D. Cox and H. Miller, The Theory of Stochastic Processes, 1965.
[8] P. Mell et al., "Common Vulnerability Scoring System," FIRST, 2007
[9] R. Böhme and G. Schwartz, "Modeling cyber-insurance," 2010.
[10] S. Romanosky et al., "Content analysis of cyber insurance policies," 2019.
[11] M. Shinohara, "Quantitative approaches to cybersecurity risk," 2013.
[12] E. Luiijf et al., "National cyber security strategies," 2014.
[13] D. Helbing, "Globally networked risks," Nature, 2013.
[14] T. Sommestad et al., "Estimating attack probabilities," IEEE TDSC, 2013.
[15] P. Embrechts et al., Modelling Extremal Events, 1997.