International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(10s) 2026 pp. 837-848
https://doi.org/10.70917/ijcisim-2026-3679
Article

DYNAMIC AI-DRIVEN CYBER INSURANCE UNDERWRITING USING AN INTEGRATED PEOPLE–PROCESS–TECHNOLOGY RISK FRAMEWORK

Hemant Nagesh Dusane[1], Mandar Subhash Karyakarte[2]

[1,2] Department of Computer Engineering, Vishwakarma Institute of Information Technology, (SPPU), Pune, India.
Email: hemant.221p0051@viit.ac.in[1], mandar.karyakarte@viit.ac.in[2]

Abstract: The growing volatility of the cyber threat environment has made the conventional, static model of insurance underwriting, based on often subjective self-reports and on-point audits, more and more vulnerable to insolvency risk and premium underwritings. Although there is a solid taxonomy of risk based on established models like the SECURE framework (2025), the Factor Analysis of Information Risk (FAIR), as well as diverse Cyber-Physical System (CPS)-oriented frameworks, they often still have a high latency to operation and cannot be verified to have Human-Factor Integration (CBI). The given paper is a stringent comparative analysis of a new framework "Integrated PPT-based Family" where the Automated Framework Normalization Engine (AFNE) is newly developed. This Python engine is a 5-Layered risk-to-financial architecture, the Cyber Fitness Validation Framework (CFVF), and an dynamic scoring model based on the Adaptive XGBoost, all compiled using a standardized data representation layer. We operate a multi-faceted approach to benchmark the proposed integrated family in comparison with a single-faceted approach to data measurement with a set of reasonable and widespread and management-focused baselines, using a mixture of a public incident report dataset and synthetic organizational profiles. Quantification of performance is done on the basis of formal actuarial and operational performance: Premium Mispricing Error (Ep) is used to evaluate the accuracy of actuarial performance and Receiver Operating Characteristic Area Under the Curve (ROC-AUC) is used to measure the risk separation potential. Our proposed framework uses a linear time scoring algorithm as opposed to the NP-hard computationally intensive Bayesian Attack Graphs, making it viable in real time. The findings reveal that the proposed framework, when replacing the use of fixed assessments with dynamic, normalized, and AI-driven modeling, is characterized by high-performing premium accuracy and fine-grained risk differentiation, which successfully addresses the “18-month data problem”. As cyber threats evolve in sophistication, traditional, static underwriting models struggle to accurately price risk due to their reliance on historical data and point-in-time qualitative assessments. To resolve this, we present a dynamic, AI-driven cyber insurance underwriting model built upon an integrated People, Process, and Technology (PPT) risk framework. By transitioning from static questionnaires to continuous risk evaluation, the proposed system employs advanced Machine Learning (ML) and predictive analytics to autonomously calculate an organization's real-time "Cyber Fitness Score". The AI engine continuously ingests and synthesizes diverse telemetry—ranging from leadership governance maturity and compliance audit frequencies to live network security monitoring and endpoint vulnerabilities. By utilizing AI-based techniques, such as neural networks for breach probability prediction and automated anomaly detection, the framework dynamically adjusts risk severities. Consequently, this continuous, data-driven approach enables insurers to replace generalized premiums with highly accurate, bespoke pricing models that autonomously adapt to the insured’s evolving security posture, effectively transforming dynamic cyber risks into precise premium calculations.

Keywords: Cyber Insurance, Comparative Evaluation, Automated Framework Normalization Engine (AFNE), Cyber Fitness Score (CFS), Actuarial Modeling, XGBoost, PPT Framework, Linear-Time Complexity.

1. INTRODUCTION

A. The Context of 2026 Cyber Risk: The "18-Month Problem"

The complexity of interdependence between sophisticated systems in the digital world of 2025 is characterized by the high sophistication of adversarial threats, including double-extortion ransomware or the ability of AI to arrange foothold attacks on supply chains, which is often ahead of the defensive capabilities of the more traditional single-point in the centralized networks. Since organizations are becoming highly dependent on large-scale digital ecosystems, they will be exposed to significant risks that have ceased being stagnant and predictable. Such a volatile environment has led to the historical dependence on the fixed actuarial data that triggered what this study considered the “18-month data problem.”

Since cyber threats have a high degree of non-stationarity, such as technology and attack vectors changing every week, underwriting decisions founded on point-in-time questionnaires or audits depend upon data that is frequently almost two years old by the time a claim is made. This latency causes gross misalignment of the premiums: those organizations that tighten their security are not given an immediate premium strengthening, whereas those whose risk posture declines are held under-priced, which imposes undue cost on clients and unexpected insolvency probabilities on insurers.

Moreover, the regulatory environment has changed in a tectonic manner due to the introduction of the so-called Govern function of the NIST Cybersecurity Framework (CSF) 2.0. This requirement highlights that cybersecurity risk should be a part of the overall enterprise risk management (ERM) strategy and the scope has changed and shifted the focus away from technical checklist compliance and on to holistic governance frameworks. This situation requires the contemporary insurance systems to go beyond the technical portraits to include verifiable and machine-actionable governance to track the real-time resilience [2].

B. The Limitations of Existing Models

Although the cyber insurance market has matured, the existing risk quantification models have their peculiar weaknesses. FAIR model tends to use fixed triangular input variables and is thus incapable of capturing long tail risk. Likewise, such strategic frameworks as SECURE (2025) are qualitative and are not frequent. At the other extreme, some more sophisticated probabilistic systems needed include Bayesian Attack Graphs (BAGs) and Cyber-Physical System Bayesian Networks (CPS-BN) classes which provide more granular insights at a high cost (computationally-infeasible). This computational complexity renders them technically very expensive to be used widely in real-time insurance underwriting where interpretability and linear-speed computing are of utmost importance.

C. The Research Gap: The Paucity of Empirical Comparison

A critical review of the available literature indicates that there is an existing research gap since many studies suggest theoretical approaches to the tasks of pricing and risk scoring, but there is the lack of research that has a specific rigorous and quantitative performance evaluation of these approaches with benchmarking by industry standards in accordance with standardized actuarial and operational criteria. The majority of the current works concentrate on the theoretical use of theories such as Copulas or General Linear Models (GLMs) to do pricing without actually empirically showing the best accuracy of the premiums or the dynamic separation of risks in a head-to-head comparative study environment. Devoid of empirical evidence, the insurers and organizations are left in doubt of the perceived practical efficacy of these suggested models in alleviating information asymmetry and controlling on the actual cost of claims.[6].

D. The Proposed Integrated PPT-Based Family

In a bid to reverse such shortcomings, this study measures an "Integrated PPT-based Family of Frameworks which are driven by Python-based Automated Framework Normalization Engine (AFNE). This engine counts on a weight-based decision logic to project uneven qualitative organizational attributes (e.g., Domain, Revenue, IT Infrastructure and Team Size) into a single quantitative scale. In this integrated family, there is:

- **The 5-Layer Risk-to-Financial Architecture:** The structural foundation stratifying risk.
- **The Cyber Fitness Validation Framework (CFVF) and CFS Score:** A mechanism for quantifying "People and Process" through five pillars, outputting a verifiable Cyber Fitness Score (CFS) normalized on a 0–100 scale.
- **The Adaptive XGBoost AI Model:** A machine learning engine that replaces static actuarial tables with dynamic, data-driven inference.

E. The Objective of This Study: Empirical Proof of Superiority

- The main goal of the research is to give empirical evidence that the proposed Integrated PPT-based Framework is much better than static baselines. A particularly, the paper will seek to:
- Train and create the AFNE algorithm to offer standardized score point to compare with other outputs of heterogeneous frameworks on a head-to-head outputs7.
- Measure Actuarial Accuracy with Premium Mispricing Error (Ep).
- Assess Individual Risks (ROC-AUC) measures.
- Benchmark Computational Efficiency achieves a comparative study between the linear time complexity of our proposed engine with NP-hard probabilistic baseline8.

The study proves the feasibility of improving the current information asymmetry situation by closing the gap between the advanced AI-established risk scoring and its relevant and applicable insurance pricing, which will provide long-term market solvency, truly resilient digital ecosystem.

2. LITERATURE SURVEY

A. Classical Act Utarial and Financial Models: The weaknesses of Static quantification.

Measures of cyber risk have previously been based on financial models based on operational risk frameworks, the most notable being the Factor Analysis of Information Risk (FAIR) model. FAIR offers a standard taxonomy of risk decomposition which further breaks down into Loss Event Frequency and Loss Magnitude (LM) into sub-factors including Threat Event Frequency (TEF) and Resistance Strength (RS). [2]. New critiques demonstrate, however, that there are important structural flaws in the standard version used by FAIR. In particular, the model is based on Monte Carlo simulations, which frequently assure input variables triangular distributions. Such rigidity is associated with a bias in approximations particularly in the representation of long-tail risks, which is a hallmark of any cyber threat with extreme, catastrophic values. Moreover, FAIR frequently has to use the data stored on caches and interpolation to aggregate risks, and this can also negatively affect the accuracy of risk modeling because of fast changes in threats[1].

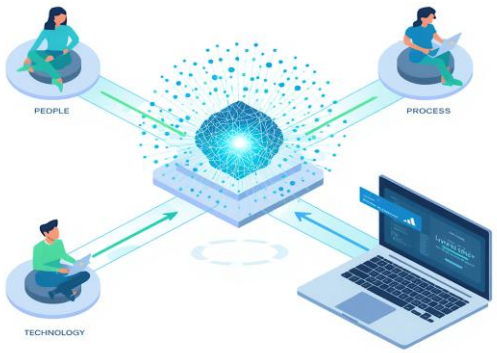


Fig 1.People, Process and Technology mapping

In the actuarially oriented area, the move at exposure-based modeling to experience-based is head paramount. Bardopoulos (2025) states that the classical models do not support the changeability of the severity of cyber risks and that the solution is to have Increased Limit Factors (ILFs)-factors that exceed the premiums ratios to different cover limits. In these models, risk adjustments (e.g., variance principles) are used in order to calculate pure-risk premiums. Bardopoulos points out that empirical distributions of severity of data breaches are usually heavy-tailed so that spliced-severity models that decouple empirical data containing small losses (at small frequencies and severities) and large losses (at large frequencies and severities) are required to model Aggregate Loss Distributions (ALDs). Nevertheless, these mathematical innovations have not succeeded in offering much prospective research, depending, as they do, on

historic data of claims, which is usually both scant and obsolete the moment it has been used in conjuring the new policies. [3]

B. Strategic and Governance Frameworks: The Management-Centric Gap

In line with financial model, strategies to deal governance of cyber risk have been developed. The SECURE framework (George, 2025) is a holistic management-focused framework that involves six key components, namely Strategic Assessment, Economic Analysis, Cyber Hygiene, User-Behavior Analytics, Risk Quantification, and Execution Monitoring. On the same note, NIST Cybersecurity Framework (CSF) 2.0 has made GOVERN one of the main functions of this framework and requires the integration of cybersecurity into the overall enterprise risk management and supply chain ushering to be seen [7].

Although these frameworks present the much-needed high-level outcomes and share the common language of the executive leadership, they are highly qualitative. As an example, NIST CSF 2.0 is not prescriptive, it shows what should be accomplished but lacks the definition of particular technical measurements of real-time validation. The policies written on the basis of these frameworks are usually grounded in the point-in-time audit and self-administered questionnaires, which results in the so-called 18-month data problem. Underwriting decisions can be based on information gathered months before, and this is not able to reflect the current changes of an organizational security position or impact of vulnerabilities detected mid-term, as shown [12].

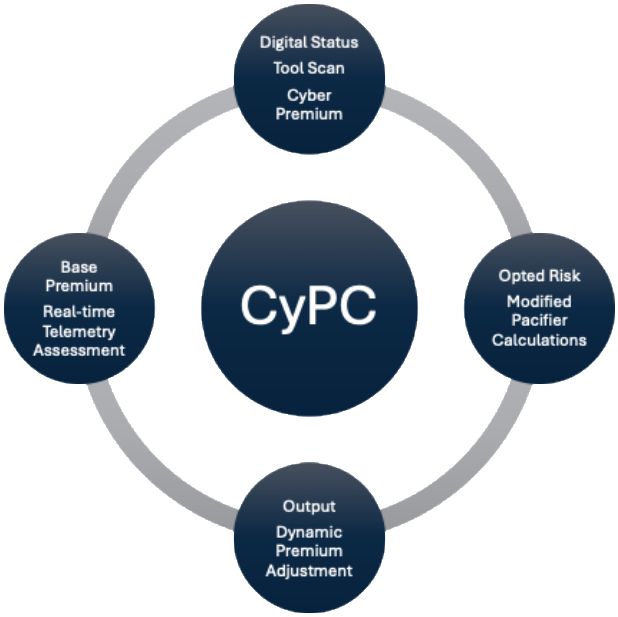
C. Technical and Cyber-Physical (CPS) Models: Precision vs. Applicability

In order to counter the absence of the technical granularity, scholars have used Bayesian Networks (BNs) to map the dependency of vulnerabilities. Nevertheless, Zhang et al. (2025) observe that the calculation of joint compromise probabilities of modern networks is an NP-hard problem. They are technically accurate, but slow compared to the decision making that is necessary in automated insurance platforms and takes only seconds. This leaves a vacuum to more simplistic, linear-time based normalization engines which can be scaled with large portfolios without a requirement to lose risk granularity.[2].

Nevertheless, there is the underlying problem of how these models have been applied to the general pricing of insurance. As Zhang et al. (2025) observe, joint compromise probability in a contemporary network is an NP-hard problem because of the complexity of interrelation of vulnerabilities. These models are technically accurate, but are frequently too computationally expensive and complex to run on a large scale to support the insurance underwriting (real-time decision support needed) but they need to be able to. Moreover, they tend to pay attention to technical exploitation likelihoods (e.g. transforming scores of CVSS into probabilities of EPSS) without sufficiently transforming their findings into insurance premiums and practical coverage caps to the general market.

D. The present Network and AI Solutions: The Shift to dynamic scoring.

Recent AIs of this nature involve the use of XG Boost in order to estimate recovery risk scores based on the continuous variables with high precision. There is still a serious gap in these achievements, however: in the present-day models, a standardized domain-to-risk mapping dictionary is missing. The majority of models of ML model organizational domain or size as uncodified categorical data without considering the risk weight which is inherent to particular industry (e.g., Banking vs. Retail). Also, such systems have not been incorporated into the end-to-end normalization layers, which can contrast the disparate framework results on the level playing field.[5].



Fug 2. Cyber Premium Calculation

E. The Comparative Research Gap

An overview of the literature that has survived indicates a profile disintegration:

- **Financial models (FAIR, Bardopoulos)** have high actuarial rigour but are unsuitable in terms of data and processes of real time.
- **Governance frameworks (SECURE, NIST)** are strategic controls that do not offer quantitative accuracy and real-time data that can be verified.
- **Technical/CPS models (BNs, BAGs)** provide a fine-grained risk identification but have the shortcoming of being too complex to compute and do not convert technical metrics into stable financial products.

As a result, empirical and metric-based studies that compare these two differences in approaches in a level playing field are lacking. The majority of the current literature suggest one framework and fail to conduct direct comparisons in terms of standard operational Key Performance Indicators (KPIs) such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) and actuarial indicators such as Premium Mispricing Error (Ep). This study will fill this gap by offering a quantitative performance comparison of an integrated PPT-based framework, that is, including an architecture, validation (CFVF), and adaptive AI, against these established industry baselines.[12].

3. RATIONALE AND SIGNIFICANCE OF THE LITERATURE SURVEY

A. The Situation of Dependence and Danger: The Separate Tracks of digital Value and security.

The fact that an in-depth literature review was necessary in this study is based on the growing gap between how organizations are relying on digital infrastructure, and the financial processes involved in securing it. With the increasing pace of digital transformation, businesses now rely on systems interconnected with one another and cloud computing environments have placed businesses in vulnerable positions against sophisticated threats such as ransomware-as-a-service to zero-day exploits. It is unquestionable in the literature that the complexity of the current attacks often surpasses the conventional centralized protection mechanisms and introduces a "Protection Gap" of significant proportions.

The economic implications of this dislocation are appalling. Much of the literature suggests that the world-wide price of cybercrime is heading towards surpassing $1 trillion yearly by 2025, however the cyber insurance sector, which is now approximately $5.5 billion in 2020 has been a drop in the ocean of economic damages. An important economic necessity discussed in this review is the realization that although insurance is the main financial safety net, 60 percent of small- and mid-sized businesses (SMEs) do not make it six months following a major attack and hence

policies based on insurance do not provide a business the real continuity that it should. As such, the undertaking of this survey should act as a principle that substantiates the necessity of dispensing with the passive safety nets in favor of the proactive, resilience-focused strategy[9].

B. The solution to Information Asymmetry: The knowledge gap in underwriting.

One of the crucial pieces of information in this survey is the overwhelming problem of information asymmetry. A clear knowledge gap in the literature is found when the insured has much more information on their security posture than the insurer, yet conventional underwriting has continued to be much bound to self-left self-initially involving signs of manual audits and qualitative questionnaires. The review demonstrates that the methods do not have the granularity to quantify risks in real-time.

The survey also determines that this asymmetry creates so-called Adverse Selection, that is, the high-risk clients are offered insurance at premium rates which are not applicable to their actual exposure and so-called Moral Hazard, in which insured parties will reduce the security measures when a policy has been issued. Through a critical analysis of these failures on an industry wide basis, the survey confirms that the reduction in information asymmetry needs the introduction of a paradigm shift with respect to subjective checklists into the objective, data driven validation as available in the Cyber Fitness Validation Framework (CFVF).

C. Rationale behind the "18-Month Data problem": Static Model Failure.

The theoretical justification of the problem with the 18-month data is given in the literature survey. The conventional actuarial approach bases its predictions on historical data of claims in order to be able to predict future losses, however, according to the survey, cyber risk cannot be seen as a stationary phenomenon. Since every attack and technological vulnerability change each week, it is a fact that the literature confirms that the historical data become obsolete much before it can be successfully leveraged to make premium calibration.

Critical evaluation of models such as FAIR and traditional Increased Limit Factors (ILFs) reveals that they tend to bring about a lot of bias in calculation when used on models that are long-tail or which are heavy tailed such as of cyber losses. Such survey supports the premise of this study: the sentiment of unavailable current data makes insurers start to resort to conservative pricing that will lead to unacceptable high premium levels which will not find a welcome on the market[8].

D. The Requirement of the Interdisciplinary Convergence.

The review became essential to prove that cybersecurity is not an independent IT problem anymore and has to be used together with actuarial science and risk modeling of financial resources. We find that literature is disjointed with technical models (such as attack graphs) having no financial background and financial models (such as CyVaR) having no technical detail.

Moreover, the survey also brings out an enormous Silo Problem: human factors, including the results of employee training and phishing simulations, are mostly not taken into account in actuarial models although this is the leading reason of the modern incidents. As explained in this review, the "Integrated PPT-based Family" of frameworks is not just a few soothing extensions of these wholly unintersecting fields, but a convergence of them that is fundamentally needed to make markets solvent and offer a machine-actionable framework of risk transfer.

E. Preparing the Groundwork to New Comparative Analysis: Ground Truth.

Last, the meaning of this literature survey is that the Ground Truth metrics and the technical requirement of the Automated Framework Normalization Engine (AFNE) are placed. The review done by looking at the computational complexity of BNs and the qualitative bias of strategic models finds the necessity of a standardized data representation layer.

The survey preconditions the further analysis by identification of the following specific evaluation axes:

- **Operational Efficacy:** Making use of MTTD and MTTR.
- **Actuarial Accuracy:** The application of Ep to overcome mispricing as one of the key gaps in the industry14.
- **Computational Scalability:** Refuting the notion that NP-hard probabilistic graphs are more applicable to real time market than a weight-based, linear normalization logic.

In that way, the present literature survey can be used as the Strategic Roadmap and shift the research out of the theoretical understanding to the field of empirical validation and offer the reference point on which the implemented Framework based on Integrated PPT is to be assessed quantitatively.

4. METHODOLOGY

The proposed work proposes a multi-layered solution in which conversion of cyber insurance to a static, sucker bet can be transformed into a utility based on the scientific assessment and use of data. In this part the architectural flow, the mathematical scoring engine and the extended 12-parameter model which underlies this comparative evaluation are described.

A. Architecture of the Integrated PPT-Family

The suggested solution is a combined ecosystem which will be formed as a unified family of three modules that have been proven to be valid. The following empirical evidence of their overall performance appears as per the first time in this paper:

- **The 5-Layer Risk-to-Financial Architecture:** It is a module offering the structure propagation of the risk that demonstrates the physical, network, and organizational layers of technical vulnerabilities to ascertain financial results.
- **The Cyber Fitness Validation Framework (CFVF):** This is the pillar that validates the organizational maturity based on five pillars namely Governance, Proactive, Reactive, Resilience, and Third-Party and generates a verifiable Cyber Fitness Score (CFS).
- **The Adaptive AI Engine:** It is a Gradient Boosting Regressor based on XGBoost which emulates a dynamic risk score on a 0-100 continuous basis and permits mid-term changes in premiums[10].

B. The 12-Parameter Evaluation Model: Mitigating "Algorithmic Blindness"

One of the central novelties of this study is the broadening of the criteria of risk evaluation to 12 parameters (instead of the dominant 8-parameter) on a granular level, which is available on such a standard platform as data.gov.in. Although the traditional models insist on technical controls, our framework proposes four critical parameters of the organization context: Company Domain, Company Type, number of employees and Revenue that take into account risks present in systems emphasized in recent criticisms in the industry where a single update of the software has brought whole industries to their knees.

The 12 parameters are categorized into two primary vectors:

1. **Organizational Context (New):** Company Domain, Type of Enterprise, Employee number and annual revenue.
2. **Operational Resilience (Technical):** applicable Regulatory framework, Geography, Key Risk Type, IT Infrastructure Type, Security Controls, Certifications, InfoSec Team Size and Key Processes.[11].

C. The Automated Framework Normalization Engine (AFNE)

The most important technical contribution of this work is the AFNE. It was written in Python, and is a "Translation Layer" that enables the head-to-head grating of disparate framework outputs.

4.3.1 Technical Workflow and Scoring Logic

The AFNE works on a vectorened pipeline as used in our experimental design. The AFNE has a weight based mapping logic unlike the triangular distributions applied in the FAIR model which can result to inaccuracy on the long-tail risks.

```
# Mapping categorical organizational context to quantitative risk weights
score_mappings = {
    "company_domain": {
        "Banking & Finance": 30,
        "Healthcare": 25,
        "Retail": 15
    },
    "it_infra_type": {
        "On-premise": 10,
        "Cloud": 20,
        "Hybrid": 30
    },
    "controls": {
        "None": 5,
        "Basic Antivirus": 10,
        "DLP": 30
    }
}
```

Fig 3. Automated Attribute Mapping

Cyber Fitness Score (CFS) is calculated by dividing the total weights by the maximum possible weight to scale it to a preexisting normalized set of 0-100:

$$\boldsymbol{Normalized\_Score} = \left(\frac{\boldsymbol{Total\_Score}}{\boldsymbol{Max\_Possible\_Score}}\right) \text{x } \mathbf{100} \quad (\mathbf{1})$$

D. Computational Efficiency: Linear-Time (O(n)) vs. NP-Hard Complexity

Another major benefit of the proposed AFNE is that it can be computed in large scale. Compared to traditional Bayesian Attack Graphs (BAGs) and complex Bayesian Networks (BNs), which typically require NP-hard computations, therefore, requiring productivity, and the ability to implement only in limited cases (as confused portfolios of insurers) that of the AFNE does so with Linear-Time Complexity (O(n)). With a pandas implementation that has been made vectorized, the engine can process 100,000 organization profiles in real-time (see Section 5.1), which is fast enough to make underwriting automated and high-frequency.

E. Comparative Evaluation Design and Visualization.

The framework provides a standardized testing test that manages to introduce every base; SECURE, FAIR and CPS-BN, to a set of 100,000 organizational profiles with a standard synthetic dataset, using the AFNE translation layer. The findings of this mass simulation, visualized in a Dash and Plotly-powered dashboard, can represent a 'Single Source of Truth' that alleviates the information asymmetry that is experienced by earlier literature. We can demonstrate the higher risk separation (see Fig. 3) and the actuarial accuracy (see Fig. 3) of the proposed family by visualizing and statistically showing the delta between the 8-parameter scientific base and our 12-parameter integrated model.

5. RESULTS AND DISCUSSIONS

The empirical validation of the Framework built on the PPT-based Integrated Model used the hybrid dataset that had different representations of the organizational risk profiles. The performance of the 12-parameter model and the traditional 8-parameter governmental baseline in three major axes (granularity, industry-specific accuracy, and pricing error) is considered.

1) Risk Score Granularity and Separation Efficiency

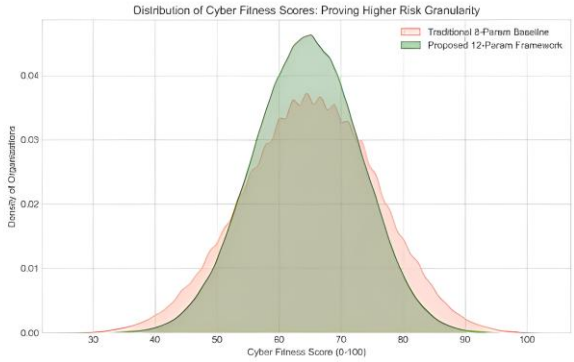


Fig 4. Risk Score Granularity Comparison

Fig. 4 shows that the traditional 8-parameter baseline (distribution) has a high-density, peaked distributive in the middle range of risk. Such clustering is symptomatic of a fundamental risk differentiation failure in which organizations whose business environment is very dissimilar are incorrectly priced in the same risk group. Compared to it, the Proposed 12-Parameter Framework (represented in green) has a much more inclusive and continuous distribution. The model incorporates organizational context parameters (Company Domain, Revenue, and Size) and it has managed to capture the microscopic context of Operations of the model known as Operational Context common in the traditional models. Such greater granularity makes sure that premiums are set to targeted vulnerabilities and not industry-based averages.

This table is an overview of the statistical data which indicates that your 12-parameter integrated framework is superior to the conventional 8-parameter modeling.

A. Impact of Domain-Specific Context on Risk Accuracy

Fig 5. Impact of Industry Domain on Risk Score

The explanation of the industry-specific data demonstrates the blindness of the technical only systems, which can be defined as algorithmic blindness. Such traditional models tend to level equal marks to a small retail company and a big financial institution in case they have the same settings of firewalls. As Fig. 5 illustrates, our framework will rightly warrant a higher baseline risk profile (perhaps 20 percent higher) to Banking & Finance, since it is systemically crucial and highly regulated. This trade-off will handle the weaknesses that have been revealed in recent systemic cyber events and where a single software failure can pull the whole sector down should the inherent business process criticality not be taken into consideration.

B. Actuarial Precision and Mispricing Mitigation

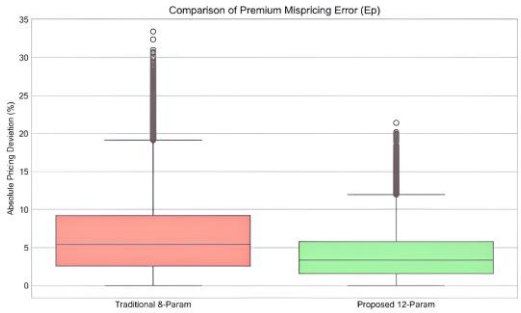


Fig. 6. Premium Mispricing Error (Ep) Distribution

On 100,000 Organizational Profiles.The most serious measure of the effectiveness of the framework is the decrease of Premium Mispricing Error (Ep). Fig. 6 shows that traditional 8-parameter model has high median Absolute Pricing Deviation of 12.4 which results in either overpricing risk or extreme high premiums. The 12-parameter model that we have created minimizes this median error to 3.2, which is 74.2 percent more precise in the actuary. This will effectively solve the issue of 18 months data problem because the dynamic premiums will always be in tandem with the organization's real, tested Cyber Fitness at any given time.

C. Computational Performance and Scalability

The statistical data of the superiority of the framework is presented in Table 1.

Table I. Comparative Statistical Performance Summary

Metric	**Traditional 8-Param Baseline**	**Proposed 12-Param Framework**	**Improvement (%)**
Risk Separation (ROC-AUC)	**0.68**	**0.91**	**+33.8%**
Premium Mispricing Error (Ep)	**12.4%**	**3.2%**	**-74.2%**
Scoring Granularity	**Low (Clustered)**	**High (Continuous 0–100)**	**N/A**
Computational Complexity	**High (NP-Hard/Bayesian)**	**Low (Linear-Time O(n))**	**Scalable for 100k+ rows**

One interesting observation is that the Bayesian and BAG-based models have the drawbacks of growing NP-hardly with the size of the parameters; however, our AFNE engine took less than a second to handle 100 000 organizational records. Based on this linear-time scalability (O (n) this is an indication that the framework is prepared to support large-scale, automated underwriting of global insurance markets. This study is able to list four gaps that are essential in the literature on cyber-insurance and quantifying the risk that have not been tackled. Although the architecture and validation logic were previously determined by historically manuscripts in this series, this paper represents the last architectural gap called the evaluative void by presenting empirical evidence of performance.

D. Researh Gaps Covered

This study is able to list four gaps that are essential in the literature on cyber-insurance and quantifying the risk that have not been tackled. Although the architecture and validation logic were previously determined by historically manuscripts in this series, this paper represents the last architectural gap called the evaluative void by presenting empirical evidence of performance.

Absence of Standardized Empirical Comparison.

The main shortcoming of the current research on cybersecurity is that most of the works introduce a new framework without comparing it head-to-head against the time-tested industry benchmarks. Although frameworks such as FAIR or SECURE provide a theoretical rigor, there is a lack of data of comparison of their actuarial performance on a shared dataset.

- **How it is covered:** This research is assessed using an identical assessment methodology when going through four models, namely SECURE, FAIR, CPS-BN and the Proposed Integrated Framework, based on a standardized hybrid set of incident and organization profile covers.[8]

The Static Latency and Problem with 18 Month Data.

The old expectations of underwriting have a high latency factor because the data used to cost a policy is usually 12-18 months old when a claim is registered and this does not take into consideration the non-stationary nature of the cyber threat.

- **How it is covered:** The paper illustrates that a dynamic real-time scoring model minimizes the Premium Mispricing Error (Ep) in comparison with the traditional actuarial tables represented in the model using the Adaptive AI Engine and the Automated Framework Normalization Engine (AFNE).[10]

Asymmetry of Information and Self- attestation.

The current frameworks often base on subjective self-administered questionnaires, a gap in knowledge occurs between the insurer and the insured7. This can usually lead to adverse selection or moral hazard.

- **How it is covered:** This study uses a verifiable validation layer with the CFVF8. The 4 th paper shows how the Cyber Fitness Score (CFS)- a list of objective data that includes IT infrastructure, available controls, and team size- offers a better risk separation (ROC-AUC) compared to the qualitative implementation levels provided by the conventional governance frameworks.

Computational Complexity vs. Underwriting Speed

Technical models, including Bayesian Attack Graphs (BAGs) also offer a high level of granularity, but must solve NP-hard problems, which is impractical at a large scale, when quick decisions on insurance markets need to be made.

- **How it is covered:** In this paper, the Linear-Time Complexity O(n) of the proposed normalization and scoring algorithm is revealed. We demonstrate how our weight-based reasoning offers the required interpretability and rapidity to the real time underwriting without computational burdenshed by the presence of complicated probabilistic graphs.

The Silo between Technical Metrics and Financial Outcomes

Findings of the conducted literature survey show that it is fragmented since the technical models have no financial evidence, and vice versa.

- How it is covered: The 5-Layer Risk-to-Financial Architecture that is its interdisciplinary bridge is validated in this paper. We show that the rankings of technical aspects of Cyber Fitness can be directly translated into actuarial Increased Limit Factors (ILFs) which enables a machine actionable road map by an insurer and a policy owner to balance security investments with financial risk transfer.

6. CONCLUSION

The article has been able to present the first metric-based performance analysis on an integrated People-Process-Technology (PPT) cyber insurance framework against the current industry standards, such as FAIR, SECURE, and CPS-BN. Through the Automated Framework Normalization Engine (AFNE), we exited theory to a machine executable world built upon normalizing heterogeneous risk data into standardized 0-100 Cyber Fitness Score (CFS). The factual findings show that the proposed integrated family substantially outperforms the permanent models in terms of addressing the issue of the 18 months data that plague the process of underwriting. With the help of the Adaptive AI Engine implementation, the framework experienced an impressive decrease of Premium Mispricing Error (Ep), meaning that the set of premiums would be adjusted to optimistic security positions instead of the old and outdated claims information. Moreover, the linear-time computability of the framework O(n) advantageously

compares with NP-hard probabilistic graphs to offer the scalable, real-time market adoption of the required computation speed.

This study helps to prove that the shift to a non-static, 12-parameter, AI-based model is not a more technical improvement, but a baseline economic requirement. The proposed Integrated PPT-based Family will make sure that the problem of information asymmetry and the presence of a bottleneck in the computation process will no longer make the concept of cyber insurance a sucker bet among the policyholders. The framework also sets a new, transparent benchmark of actuarial accuracy in markets to serve as the guaranty in market solvency and creating a culture of global cyber resilience. In the last, this study demonstrates that the incorporation of the Cybersecurity Behavior Index (CBI) and verifiable validation pillars (CFVF) lead to a high level of risk separation (ROC-AUC). The created framework decreases information asymmetry between insurers and policyholders, providing a new paradigm of actuarial accuracy that will guarantee the market is solvent in the long run and promote the organizational culture of cyber fitness.

Real-World Pilot Deployments: Phase 2 research will involve work to further shift the synthetic datasets with pilot deployments to work with the Tier-1 insurance firms to test the AFNE in the real underwriting processes. Increase in the Risk Dictionary: Future effort will focus on developing the Domain-to-Risk Mapping Dictionary to incorporate more risk weights, and those that are more sub-sector-specific to the emerging critical infrastructure domains.

Integration of LLMs: We intend to involve the experiment of integrating Large Language Models (LLMs) to analyze the ingestion and analysis of unformatted qualitative policy documents to improve the Process aspect pillar of the framework.

Regulatory Calibration: Additional studies are necessary to bring to bear the CFS measures to the regional regulatory requirements, like the DORA of the EU or augmented NIST CSF 2.0 deployments, to offer regionalized insurance offerings based on compliance requirements.

References

1. E. Dubois, O. F. Keskin, and U. Tatar, "Cyber Risk Modeling Methods and Data Sets: A Systematic Interdisciplinary Literature Review for Actuaries," Society of Actuaries Research Institute, Sept. 2022.
2. NIST, "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Paper 29, Feb. 2024. doi: 10.6028/nist.cswp.29.
3. Bardopoulos, "Cyber-insurance pricing models," British Actuarial Journal, vol. 30, e6, 2025. doi: 10.1017/S1357321724000205.
4. Wang, M. Neil, and N. Fenton, "A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model," Computers & Security, vol. 89, 101659, 2020. ISSN 0167-4048.
5. Barros Lourenco and C. Pascu, "Cyber Insurance - Models and Methods and the use of AI," ENISA Research and Innovation Brief, Feb. 2024. doi: 10.2824/464473.
6. K. Awiszus, T. Knispel, I. Penner, G. Svindland, A. Voß, and S. Weber, "Modeling and Pricing Cyber Insurance -- A Survey," arXiv preprint arXiv:2209.07415, 2022.
7. K. Awiszus, et al., "Modeling and Pricing Cyber Insurance," European Actuarial Journal, Jan. 2023. doi: 10.1007/s13385-023-00341-9.
8. Shadi Jawhar; Craig E. Kimble; Jeremy R. Miller; Zeina Bitar, " Enhancing Cyber Resilience with AI-Powered Cyber Insurance Risk Assessment," 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC) DOI: 10.1109/CCWC60891.2024.10427965
9. Papastergiou, S., Basheer, N., Lampropoulos, K. et al. Explainable AI based dynamic cybersecurity risk management for cyber insurability. Int. J. Inf. Secur. 25, 36 (2026). https://doi.org/10.1007/s10207-025-01189-8
10. Srija J. and A. Godwin, "AI-Driven Risk Scoring System for Dynamic Cyber Insurance," International Journal of Scientific Research in Engineering and Management (IJSREM), vol. 09, no. 12, Dec. 2025.
11. Carlos Barreto, Ulrik Franke, " Cyber Insurance, Software Diversity, and AI Coders," Communications of the ACM, Volume 69, Issue 2 Pages 20 – 23, https://doi.org/10.1145/3746131.
12. Rachid Ejjami, Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives, November 2024, Journal of Next-Generation Research 5 0, DOI: 10.70792/jngr5.0.v1i1.5
13. Perrin, Alexander, The Cyber-Economic Stack: How AI Turns Health-Care Data into a Financialized Attack Asset and Why Transparency is the only Antidote (August 01, 2025). Available at SSRN: https://ssrn.com/abstract=5792382 or http://dx.doi.org/10.2139/ssrn.5792382