Cyber Risk Pricing: Current Challenges and the AI-Driven Future

Maochao Xu

Department of Mathematics
Illinois State University
mxu2@ilstu.edu

June 2026

Cyber Incident and Cost Trends (2025)

- **Incident Volume (2025 YTD):**
  - ITRC reports **2,563 incidents** in first 9 months.
  - Impacting approx. **202 million** victim notices [1].
- **Financial Impact by Region:**
  - Global Average Cost: **$4.44 million** (decreased 9%).
  - **United States Average: $10.22 million** (Record High) [2].
- **Cost Disparity by Size (NetDiligence Study) [3]:**

Metric	SME	Large Enterprise
Avg. Incident Cost	$264,000	$10.3 Million
Business Interruption	$1.8 Million	$36.1 Million

Sources: [1] ITRC Q3 2025 Analysis, [2] IBM Cost of a Data Breach Report 2025, [3] NetDiligence Cyber Claims Study 2025

Cyber Insurance Market Overview

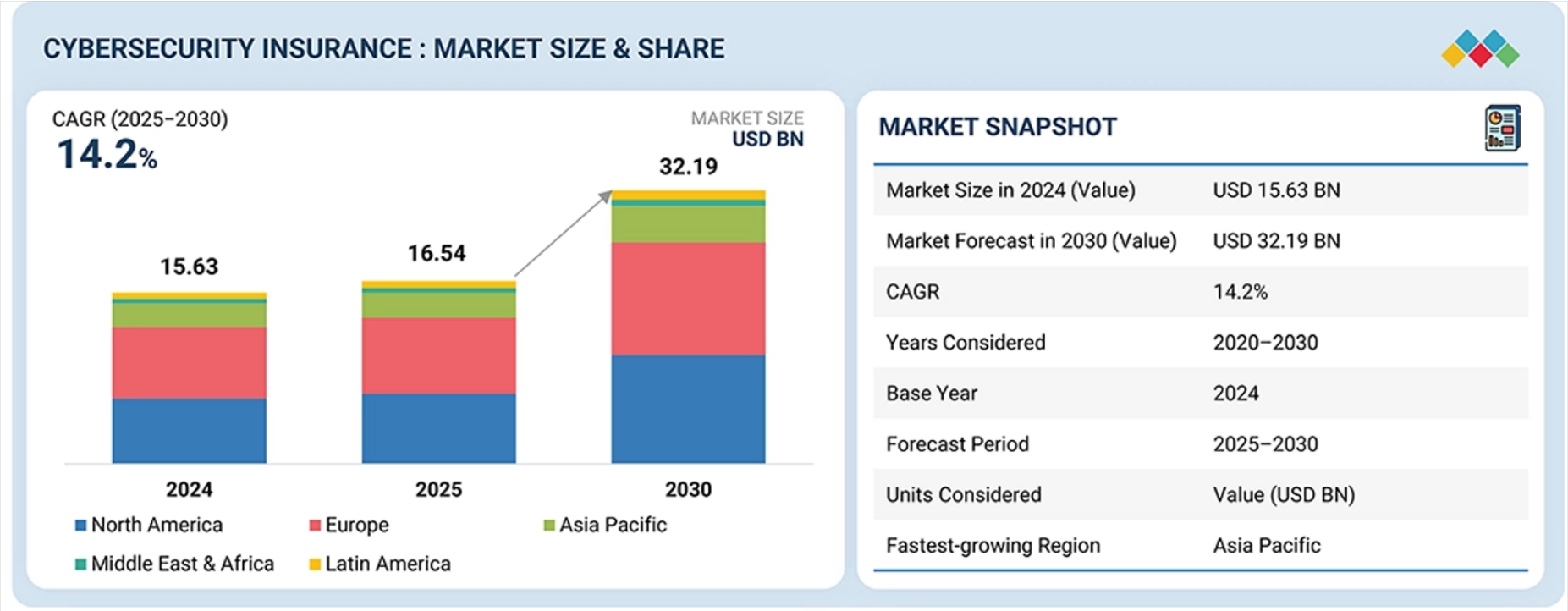


Figure: Cyber insurance market. Source: MarketsandMarkets.

NACIS 2025: Global premiums reached nearly **$15 billion**. North America: 64.9%

Top 20 companies in US

2024 Rank	2023 Rank	Group Name	Direct Written Premium	Loss Ratio with DCC	Market Share	Cumulative Market Share
1	1	Chubb Lt Grp.	$560,634,065	36.06%	7.92%	7.92%
2	4	St Paul Travelers Grp.	$535,426,655	53.97%	7.56%	15.48%
3	3	Fairfax Financial	$360,580,980	39.66%	5.09%	20.58%
4	5	Tokio Marine Holding Inc.	$355,982,823	43.47%	5.03%	25.60%
5	2	AXA Ins. Grp.	$340, 448,442	36.03%	4.81%	30.41%
6	7	Arch Ins. Grp.	$285,033,459	41.67%	4.03%	34.44%
7	32	At Bay Specialty Ins. Grp.	$280,601,661	55.78%	3.96%	38.40%
8	8	American Intrnl. Grp.	$276,564,105	49.26%	3.91%	42.31%
9	9	Sompo Grp.	$262,732,079	57.84%	3.71%	46.02%
10	10	Starr Grp.	$255,087,002	96.26%	3.60%	49.62%
11	11	CNA Ins. Grp.	$240,279,671	74.84%	3.39%	53.02%
12	14	AXIS Capital Grp.	$204,589,956	26.73%	2.89%	55.91%
13	18	AmTrust Financial Serv. Gr.	$202,476,467	48.33%	2.86%	58.77%
14	6	Berkshire Hathaway	$187,578,016	85.72%	2.65%	61.42%
15	16	Hartford Fire & Cas Grp.	$185,549,193	11.53%	2.62%	64.04%
16	19	Beazley Grp.	$184,854,545	9.24%	2.61%	66.65%
17	28	QBE Ins. Grp. Ltd.	$184,062,830	89.31%	2.60%	69.25%
18	15	Liberty Mut. Grp.	$169,793,294	70.72%	2.40%	71.65%
19	13	Zurich Ins. Grp.	$168,205,234	78.31%	2.38%	74.03%
20	17	Ascot Ins. US Grp.	$156,769,170	45.19%	2.21%	76.24%

Figure: DWP and loss ratios for the top 20 insurer groups.

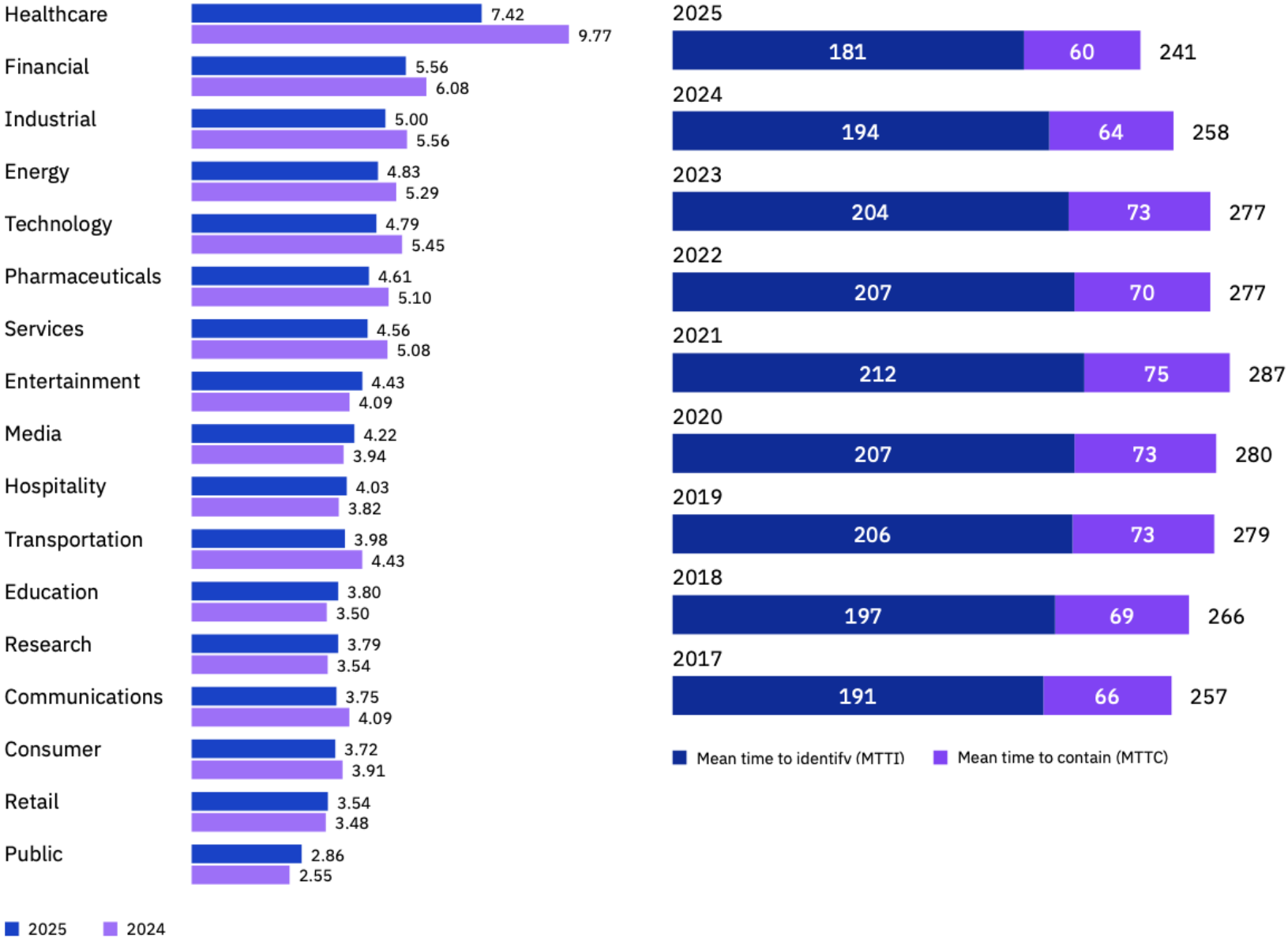
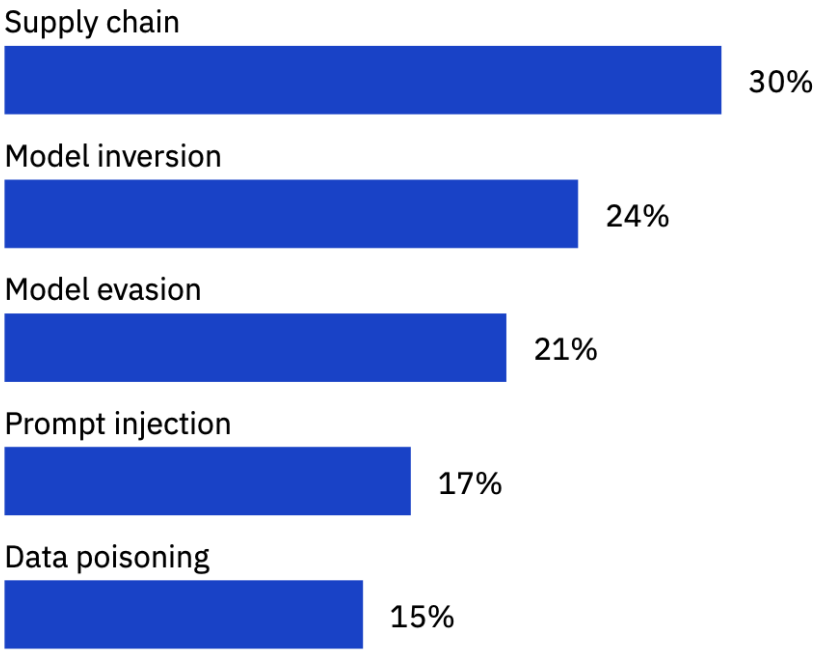
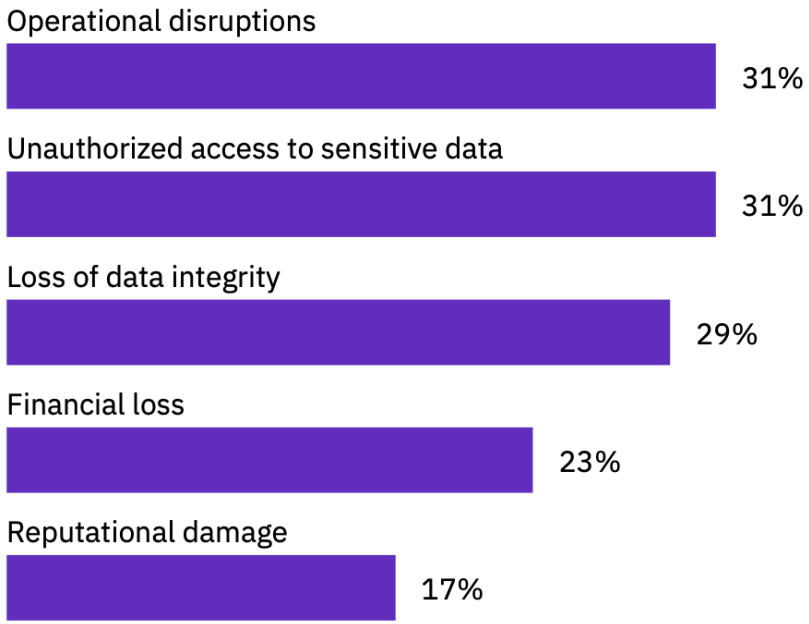


Figure: Healthcare is still the costliest sector, while response times are improving

AI Risk?



(a) Incidents involving AI models



(b) Impacts of incidents on authorized AI

Figure: AI exposure is not confined to one deployment mode, which complicates cyber underwriting and vendor-risk assessment. Future cyber pricing may need separate loadings for AI governance, vendor dependence, and internal model deployment choices. Examples: 2024–Chatbot misinformation: Air Canada; 2023–Confidential data leakage: Samsung and ChatGPT.

Why is cyber risk pricing uniquely hard?

Fast-moving threats

Attack patterns, tools, and exposures evolve faster than annual underwriting cycles.

Interdependence and accumulation

Shared cloud, software, vendors, and service providers can turn one event into many correlated claims.

Sparse and shifting loss data

Claims histories are limited, policy terms change over time, and observed losses reflect a changing market.

Heavy-tailed losses

Rare but severe incidents dominate capital requirements and pricing, yet are the hardest to calibrate.

Cyber pricing is difficult because insurers must price evolving threats with limited data while accounting for portfolio-wide accumulation from shared vendors, cloud platforms, and software dependencies.

How cyber risk is priced today

In practice, cyber pricing is a triangulation problem.

Insurers combine exposure data, security signals, scenarios, and underwriter judgment.

Exposure view

Uses size, sector, revenue, records, vendors, and core controls.

Limitation:often proxy-heavy and backward-looking.

Security view

Uses scans, questionnaires, security ratings, and control evidence.

Limitation:may miss internal context and control quality.

Scenario view

Stress-tests ransomware, outage, breach, cloud, and vendor events.

Limitation:depends on assumptions and expert judgment.

Cyber premiums are built from multiple noisy signals and adjusted for limits, exclusions, accumulation, and portfolio appetite.

How cyber risk is priced in practice

Evidence from public rate filings: cyber pricing is usually implemented through rating algorithms, rather than one universal actuarial model.

Pricing	Stylized formula	Interpretation
Flat rate	$P_c = \frac{q_c s_c}{1-\ell}$	Fixed premium for coverage c, based on assumed frequency q_c, average severity s_c, and loading ratio ℓ.
Hazard group	$P_i = P_{h(i),c,L,R}$	Premium selected from a filed table by hazard group $h(i)$, coverage c, limit L, and retention R.
Base rate	$P_i^{\text{base}} = BP_i F_{\text{limit}} F_{\text{retention}} F_{\text{industry}}$	Exposure-based base premium adjusted by limit, retention, and industry factors.
Risk modifiers	$P_i = P_i^{\text{base}} \prod_{k=1}^{K} F_{ik}$	Claims history, security controls, governance, policy terms, and sublimits enter as rating modifiers.

Public SERFF-style filings suggest cyber pricing is often table-driven, with increasing refinement from flat rates to exposure-based formulas with underwriting modifiers. These are representative rating structures; actual carrier models are proprietary and vary by insurer.

Unifying representation of filed rating algorithms

$$P_i^* = \sum_{j \in \mathcal{C}} \left[BP_{ij} \prod_{k=1}^{K_j} F_{ijk} \right] \times F_i^{\text{discount}} \times F_i^{\text{policy term}}.$$

$$P_i = \max\{P_i^*,\ P_i^{\min}\} + S_i.$$

Component	Meaning
$j \in \mathcal{C}$	Coverage modules, such as third-party liability, first-party incident response, cyber crime, system interruption, or extortion.
BP_{ij}	Base premium for firm i and coverage module j.
F_{ijk}	Rating factors such as limit, retention, industry, claims history, data classification, security controls, governance, sublimits, or retroactive date.
$P_i^{\min}$	Minimum premium floor, applied after the calculated premium is obtained.
S_i	Explicit surcharge or fee, if separately applied.

How scenario models affect firm-level pricing

Scenario models are usually portfolio-level tools used to assess accumulation, capital, reinsurance, and capacity.

$$P_i = P_i^{\text{account}} + \lambda_i^{\text{acc}}, \qquad \lambda_i^{\text{acc}} \propto \rho(L_{\text{port}} + L_i) - \rho(L_{\text{port}}).$$

In practice, the scenario load may appear as:

higher premium or lower limit or higher retention or sublimits/exclusions.

Portfolio finding	**Possible underwriting response**
High cloud/vendor concentration	Higher accumulation load, lower offered limit, or stricter vendor exclusions.
High ransomware aggregation	Higher retention, tighter ransomware sublimit, or stronger control requirements.
High business interruption tail	Higher BI rate, waiting period, sublimit, or coinsurance adjustment.
High reinsurance/capital cost	Higher technical price, capacity reduction, or portfolio rebalancing.
Diversifying account	Smaller accumulation load or more favorable capacity.

Scenario pricing asks whether this firm increases the insurer's exposure to shared cloud providers, software vendors, MSPs, ransomware waves, or other systemic cyber events.

Where current cyber pricing approaches fall short

Dynamic threat environment
Point-in-time assessments decay quickly as attackers, tools, vulnerabilities, and exposures evolve.

Systemic accumulation risk
Cloud, software, vendor, and managed service provider dependencies can turn one event into many correlated claims.

Extreme-loss tails
Rare but severe cyber events matter most for capital, reinsurance, and pricing discipline.

Sparse data and reporting bias
Claims data are limited, while insured populations, policy wording, and control standards keep changing.

Pricing errors are most costly when rare events become portfolio-wide losses.

Research 1: online probabilistic cyber risk updating

A framework for sequentially updating cyber breach frequency and severity as new incidents or risk signals arrive.

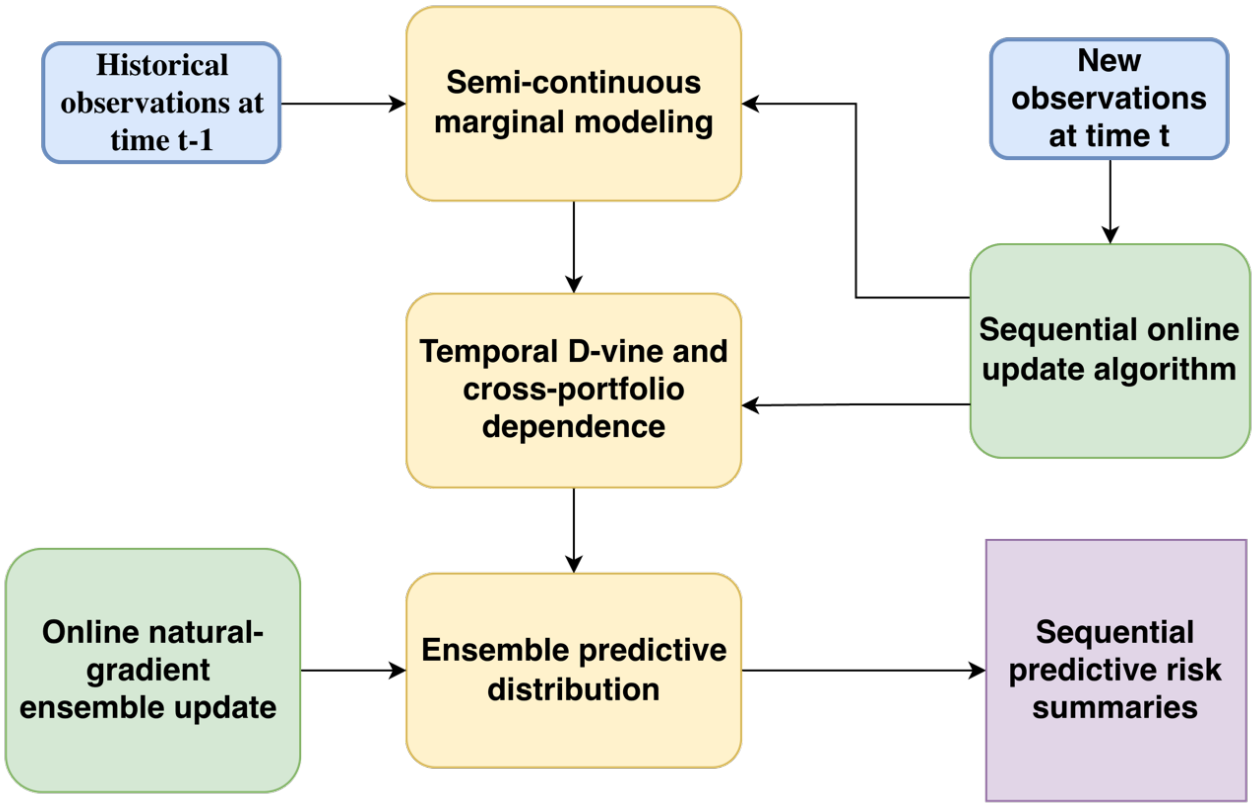
$$\widehat{F}_{i,t}(y) = \Pr(Y_{i,t+1} \leq y \mid \mathcal{D}_t, \mathbf{x}_{i,t}, \mathbf{z}_i).$$

- Cyber risk changes faster than traditional pricing and renewal cycles.
- The model produces predictive distributions, not only point estimates.
- Updated risk indications can support renewal pricing, monitoring, capital analysis, and portfolio steering.

Research outcome: sequential cyber risk modeling pipeline

What the algorithm does

- Uses historical observations to initialize marginal and dependence models.
- Incorporates new observations through sequential online updates.
- Produces predictive distributions for underwriting and portfolio monitoring.



Research 2: dependence-aware dynamic loss modeling

A deep-learning framework that captures temporal dependence, cross-group dependence, and nonlinear loss distributions for cyber risk prediction.

$$L_{\text{port},t} = \sum_{g=1}^{G} L_{g,t}, \qquad (L_{1,t}, \ldots, L_{G,t}) \text{ are modeled as dependent.}$$

How dependence is captured in the architecture:

- **Temporal attention** learns persistence and changing risk patterns over time.
- **Sector/context embeddings** allow risks to differ across industries or groups.
- **Cross-group attention** captures co-movement across related groups.
- **Mixture distribution output** represents heavy tails, zero inflation, and predictive uncertainty.

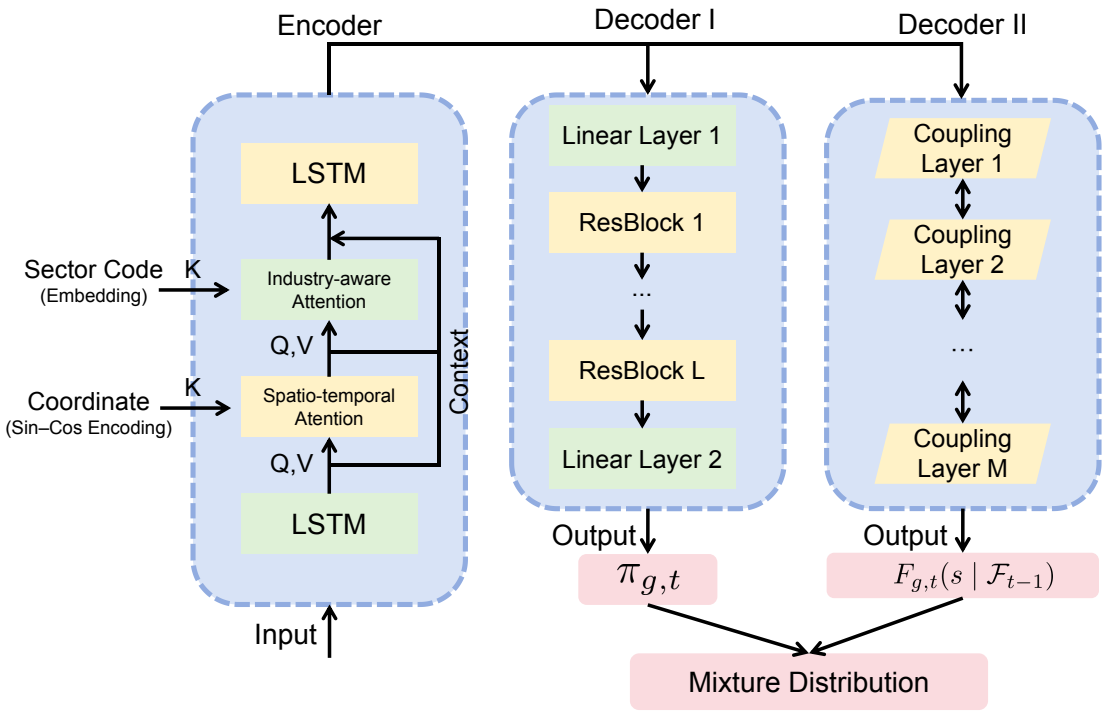
Deep learning framework: CADA-Flow

Inputs and context. Historical cyber observations are combined with sector and time information.

Encoder. LSTM and attention layers summarize temporal patterns and cross-sector context.

Decoder I. Estimates the occurrence probability, or equivalently the zero-mass component, for sparse cyber incidents.

Decoder II. Uses a context-conditioned RealNVP flow to model the conditional copula and nonlinear dependence among positive losses.



Toward next-generation cyber insurance

Future scenario: a continuous stack linking cyber telemetry, residual-risk quantification, technical pricing indications, policy support, and auditable settlement.

What changes versus today: cyber insurance moves from a static (semi-)annual quote toward a monitored, control-aware product where telemetry informs underwriting, renewal pricing, capacity, client alerts, and portfolio steering.

Near-term product design

Practical product design

Embedded monitoring + insurance subscription

Near-term deployable

Continuous sensing in the background; governed repricing in the foreground.

Core idea: bundle monitoring, prevention support, and risk transfer into a monthly service model rather than a static annual quote.

1 Continuous monitoring
IDS / EDR / SIEM signals and external scans feed a continuously updated cyber state.

2 Residual risk scoring
Convert telemetry into expected loss, tail risk, and a stable risk band that underwriters can explain.

3 Scheduled repricing
Charge a monthly fee with scheduled adjustment windows; do not change premium on every alert.

4 Shared workflow
Use the same signal stack for underwriting, client alerts, security intervention, and renewal repricing.

How the product works

Telemetry intake
Network flow, IDS/EDR, vulnerability scans, third-party signals, and external threat context

↓

Residual risk model
Estimate expected loss, tail risk, and a stable risk band rather than reacting to every alert

↓

Governed subscription pricing
Translate the risk band into a monthly fee with pre-defined adjustment windows and guardrails

↓

Coverage + service actions
Deliver insurance coverage, remediation nudges, client alerts, endorsements, and renewal repricing

Best fit: SMEs, MSSP / broker partnerships, and embedded cyber products.

Conclusion

- **Current pricing practice** provides the foundation: rating tables, exposure measures, policy terms, and underwriting modifiers.
- **AI can expand the information frontier** by transforming telemetry, threat intelligence, security controls, and claims signals into continuously updated risk indicators.
- **The modeling challenge** is to make these indicators actuarially useful: predictive loss distributions, tail-risk measures, dependence assessment, and explainable technical premium indications.
- **The future product** is AI-assisted underwriting, prevention, capacity steering, portfolio monitoring, and governed pricing review.

Cyber insurance is entering a new AI-enabled era: from static risk transfer to adaptive cyber risk intelligence.

Thank you!