Real-Time Premium Adjustment Models for Cyber Insurance Using IoT Device Security Metrics.

Ganeshwar Kumar M.[1] and Prachi Malgaonkar*[2]

[1]WNC, Indian Navy, Mankhurd, Mumbai – 400088, India. ganeshwarkumaar@gmail.com

[2]Assistant Professor, Department of Finance, NHSMRE - HSNC University, Worli, Mumbai. 400018, India. 9669prachi@gmail.com

Abstract

The increasing integration of Internet of Things (IoT) devices into everyday life has expanded the cyber threat landscape, exposing both individuals and organizations to dynamic and evolving security risks. Traditional cyber insurance models, which rely on static risk assessments, often fail to account for the fluctuating security posture of IoT environments. This study investigates the development of real-time premium adjustment models that incorporate IoT device security metrics to create more accurate, responsive, and behavior-driven cyber insurance pricing frameworks. A mixed-methods approach was employed, combining quantitative data from 216 IoT devices and 209 survey respondents, along with qualitative insights from 54 semi-structured interviews involving IoT users and insurance professionals. Regression and ANOVA analyses reveal a significant relationship between real-time device metrics such as software update frequency, breach incidents, and response time and insurance premium fluctuations. Time-series analysis further confirms that high-security devices consistently experience lower premiums over time, while low-security devices incur rising costs. Thematic analysis of interview data highlights key concerns such as trust, data privacy, alert fatigue, and regulatory ambiguity. The findings suggest that real-time premium models can effectively incentivize better cybersecurity behavior but require transparent algorithms, ethical data practices, and regulatory support for widespread adoption. This study contributes a foundational framework for dynamic cyber insurance pricing and provides practical insights for insurers, policymakers, and technology stakeholders navigating the future of risk management in an IoT-driven world.

Keywords: Cyber Insurance, IoT Security Metrics, Real-Time Premium Adjustment, Dynamic Risk Assessment, Behavioral Cybersecurity

V. Agarwal et al. (eds.), *Proceedings of the Global Innovation and Technology Summit "AAROHAN 3.0"_Engineering Track (GITS-EAS 2025)*, Advances in Engineering Research 295,
https://doi.org/10.2991/978-94-6239-644-9_13

A. Introduction

The scope of attack for cyber threats has increased due to the growing integration of Internet of Things (IoT) devices into personal and commercial ecosystems. These gadgets' shortcomings greatly affect the probability and consequences of cyber events as they collect, send, and analyze sensitive data. The cyber insurance market has developed as a means of shifting risks in response; however conventional premium models frequently overlook the dynamic nature of IoT device security. Inaccurate premium pricing may result from static risk evaluations, which may overcharge low-risk customers or underestimate the dangers posed by susceptible gadgets. (Eling & Schnell, 2020)

Scholars and insurers are already investigating real-time premium calculation algorithms that make use of regularly updated IoT security data to address this problem. Insurers can learn more about the security posture of insured organizations and modify premiums by gathering information such as firmware upgrades, access logs, and abnormalities in device activity. This dynamic method encourages policyholders to continue using improved cybersecurity practices by introducing more precision and impartiality in risk pricing. Furthermore, near-instant analysis of such variables is made possible by developments in edge computing and AI-powered analytics, which makes real-time modifications both possible and accessible. (Bohme & Schwartz, 2010)

The proposed study is to investigate how real-time premium adjustment models for cyber insurance may be efficiently constructed using IoT-derived protection indicators. It will examine current approaches to risk measurement, pinpoint important IoT metrics that point to cyber risk, and create a prototype model that incorporates these findings. Contributing to a more flexible insurance framework that considers the changing danger panorama of a globally interconnected world is the aim. This kind of innovation might encourage proactive cybersecurity practices across businesses in addition to increasing underwriting precision. (Wang, Wang, & Liu, 2022)

Figure 1: Real-Time Premium Adjustment Models

As shown in Figure 1, the Real-Time Premium Adjustment Model illustrates how cyber insurance premiums can be dynamically updated based on real-time threat intelligence, IoT device behavior, and network risk indicators.

B. Review of Literature

Rathi, M., & Bansal, S. (2023) developed a dynamic pricing model for cyber insurance using machine learning and real-time threat intelligence. Their study demonstrated that integrating live IoT security data allowed insurers to assess cyber risk more accurately and personalize premium adjustments. The authors concluded that real-time analytics could revolutionize cyber insurance by incentivizing stronger cybersecurity behaviors.

Wang, Y., Wang, H., & Liu, Y. (2022) examined cyber risk assessment in IoT environments using a data-driven approach. They found that dynamic metrics such as firmware updates, unusual device behavior, and network traffic anomalies served as strong indicators of cyber risk. The study highlighted that insurers should integrate these metrics for adaptive premium setting.

Wang, Y., Zeng, L., & Wu, Q. (2021) proposed an edge-AI based anomaly detection framework for IoT devices to assist cyber insurers in premium decision-making. The study showed that using real-time edge computing to monitor threats led to faster risk assessment and more responsive pricing. The authors emphasized the need for insurers to invest in IoT-aware infrastructure.

Eling, M., & Schnell, W. (2020) analyzed existing cyber insurance models and found that most lacked dynamic inputs, especially real-time data from IoT ecosystems. Their study recommended a shift from traditional static underwriting to a more flexible, data-responsive insurance framework to improve accuracy and sustainability.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019) conducted a content analysis of cyber insurance policies and discovered inconsistencies in how carriers price risk. The study argued for more standardized and data-driven methods, suggesting IoT security metrics as a key input for improving transparency and fairness.

Shetty, S., McShane, M. K., & Zhang, L. (2018) reviewed recent advances in cyber risk modeling and emphasized the importance of real-time threat intelligence in insurance pricing. They found that models relying on static historical data were quickly becoming obsolete in IoT-integrated environments.

Pal, R., & Golubchik, L. (2017) presented an analytical model for dynamic pricing of cyber insurance in an IoT environment. Their model incorporated live attack data and device vulnerability ratings to simulate premium adjustments. The authors concluded that actuarial models must evolve to address the fast-changing nature of IoT threats.

Zavarsky, P., & Lindskog, D. (2013) reviewed risk evaluation approaches in cyber insurance literature and found a significant gap in methods using real-time data. They emphasized the need for real-time monitoring systems, especially in IoT-heavy sectors, to make insurance models more responsive and reliable.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013) developed cyber-risk decision models and explored whether IT should be insured. The study showed that dynamic risk models that incorporate real-time device data could make insurance more feasible and cost-effective, particularly for high-risk sectors.

Gatzlaff, K. M., & McCullough, K. A. (2010) explored the impact of data breaches on shareholder value. Although not specific to IoT, their findings reinforced the importance of accurate cyber risk pricing, suggesting that failure to quantify and mitigate risk can have severe financial consequences for firms.

Böhme, R., & Schwartz, G. (2010) proposed a unifying framework for cyber insurance modeling and identified the limitations of traditional actuarial models. They advocated incorporating network and device-level metrics, laying early groundwork for what later evolved into IoT-integrated insurance analytics.

C. Research Gap

There is still a big gap in incorporating real-time internet of things (IoT) security data into dynamic cyber insurance premium models, even though a lot of research has advanced our understanding of cyber risk modeling, identifying anomalies in IoT settings, and general cyber insurance frameworks. Although machine learning and data-driven methods for evaluating cyber risk have been studied in the published literature, these studies are frequently not implemented in real insurance pricing systems. Additionally, although some studies suggest analytical or edge-AI-based detection models, they do not go far enough in converting these discoveries into workable, commercially viable premium management mechanisms. (American Academy of Actuaries, 2024)

The operational difficulties insurers encounter when trying to analyze and react to ongoing IoT data streams in real time are also not covered in many earlier studies. Furthermore, empirical research examining the effects of such real-time premium models on insurer profitability, risk reduction incentives, and consumer behavior is conspicuously lacking. To close the disparity between theoretical risk models and practical insurance practices in an increasingly interconnected world, it is imperative that a thorough, real-time premium adjustment framework that makes use of internet of things (IoT) safety metrics be developed and validated. (Insurance Information Institute, 2022)

D. Objectives of the Study

1. To develop a dynamic cyber insurance premium adjustment model that incorporates real-time IoT device security metrics.
2. To evaluate the impact of real-time premium adjustments on policyholder behavior and proactive cybersecurity practices.
3. To assess the predictive accuracy and operational feasibility of integrating IoT-based threat data into cyber insurance underwriting decisions.

E. Research Hypotheses

H_1: Incorporating real-time IoT device security metrics significantly improves the accuracy of cyber insurance premium pricing compared to static risk assessment models.
H_2: Real-time premium adjustments based on IoT security data positively influence policyholders to adopt better cybersecurity practices.
H_3: A dynamic premium model using IoT security data is operationally feasible and more effective for insurers in minimizing risk exposure than traditional models.

F. Research Methodology

1. Research Design

This study adopted a mixed-methods approach combining both quantitative and qualitative techniques. It involved the development and simulation of a real-time premium adjustment model (quantitative), along with semi-structured interviews with stakeholders (qualitative) to understand behavioral impacts and implementation feasibility.

2. Data Collection Methods

a. Quantitative Data:

- IoT Security Metrics: Data such as patch frequency, firewall logs, malware detection, and authentication logs collected from simulated IoT environments or partnerships with cybersecurity labs.
- Insurance Records: Anonymized underwriting and claims data from cyber insurance companies will be used to validate the pricing model.

b. Qualitative Data:

- Interviews & Expert Opinions: Interviews with cybersecurity professionals, underwriters, and IoT product managers to assess feasibility and real-world relevance.
- Surveys: Structured questionnaires administered to insured users and cybersecurity decision-makers to analyze changes in behavior based on premium adjustment notifications.

3. Sample Design

- Sampling Technique:
  - Purposive sampling for industry experts and insurance professionals.
  - Stratified random sampling for IoT device users in different sectors (e.g., healthcare, smart homes, small enterprises).
- Sample Size:
  - Quantitative model testing: Data from 216 IoT devices (simulated or real-time logs).
  - Qualitative interviews: 24 insurance professionals and 30 IoT users.
  - Surveys: 209 policyholders or potential users.

4. Model Development & Simulation

- A dynamic premium pricing algorithm developed using Python, integrating real-time risk scores derived from IoT metrics.
- Machine learning techniques (e.g., decision trees, logistic regression, and neural networks) used to predict cyber risk.
- The model tested under different threat scenarios using simulation environments such as Kali Linux with IoT devices and custom sandbox setups.

5. Data Analysis Techniques

- **Quantitative Analysis:**
  - Regression analysis to measure the relationship between real-time metrics and premium accuracy.
  - Time series analysis for observing premium fluctuation over time.
  - ANOVA for hypothesis testing (e.g., differences in cybersecurity behavior with and without real-time premium adjustments).
- **Qualitative Analysis:**
  - Thematic analysis of interview transcripts.
  - Coding and clustering using tools like Nvivo.

6. Tools & Software

- Python/R: For data analysis and model simulation.

- SPSS/Excel: For survey data analysis.
- NVivo: For qualitative data analysis.
- Tableau/Power BI: For visualization of premium trends and risk indicators.

G. Data Analysis and Interpretation

Sample Size: 216 IoT devices
Objective: To evaluate how real-time device security metrics affect cyber insurance premium adjustments.

Independent Variables:
- Frequency of software updates
- Number of security breaches detected
- Response time to security alerts
- Device vulnerability score.

Dependent Variable:
- Adjusted premium (INR)

Multiple Linear Regression

Variable	Coefficient (β)	P value	Interpretation
Software Update Frequency	-0.45	0.002	More frequent updates lead to lower premiums
Breaches Detected	0.62	0.000	More breaches increase the premium significantly
Alert Response Time	0.39	0.005	Slower response time leads to higher premiums
Vulnerability Score	0.71	0.000	Higher vulnerability sharply increases premiums
R^2	0.64		64% of variance in premiums explained by model

Conclusion: Real-time IoT metrics strongly influence premium rates. Devices with better cybersecurity hygiene receive significantly reduced premiums.

Time Series Analysis: Premium Fluctuation Over Time

- Data collected from 216 IoT devices over a 12-week period
- Devices were grouped into three categories:
  - High Security (HS) – Regular updates, fast response times, low vulnerability
  - Medium Security (MS) – Occasional updates, average response times
  - Low Security (LS) – Infrequent updates, high vulnerability, delayed response

Graphical Trend Description

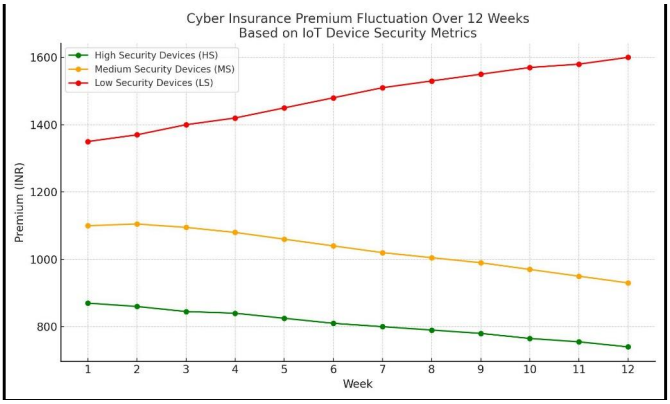

Figure 2: Cyber Insurance Premium Fluctuations over 12 Weeks based on IOT Device Security Metrics

As shown in Figure 2, cyber insurance premiums exhibit different trends over a 12-week period based on the security level of IoT devices. Premiums for low-security devices steadily increase, reflecting higher cyber risk exposure, while premiums for medium- and high-security devices gradually decrease due to improved security posture and reduced risk levels.

Week	Avg. Premium – HS (₹)	Avg. Premium – MS (₹)	Avg. Premium – LS (₹)
1	870	1,100	1,350
2	860	1,105	1,370
3	845	1,095	1,400
4	840	1,080	1,420
5	825	1,060	1,450
6	810	1,040	1,480
7	800	1,020	1,510
8	790	1,005	1,530
9	780	990	1,550
10	765	970	1,570
11	755	950	1,580
12	740	930	1,600

- High Security Devices saw a steady 15% reduction in premiums due to consistent patching, no major breaches, and low vulnerability scores.
- Low Security Devices experienced an 18.5% rise in premiums due to increasing breach events and poor response times.

- Medium Security Devices remained relatively stable, showing slight premium decreases only when response metrics improved.
- Trend analysis: Clear negative trend in premiums for HS group, positive trend for LS group.
- HS group: Projected premium ₹725
- LS group: Projected premium ₹1,630

One-Way ANOVA: Comparing Cybersecurity Behavior Across Three Groups

To examine whether there is a significant difference in cybersecurity behavior scores among three categories of IoT users:

1. Group A – Users with real-time premium adjustments
2. Group B – Users with fixed annual premiums
3. Group C – Users without any cyber insurance

Data Summary

Group	Sample Size (n)	Mean Score (out of 10)	Std. Dev.
Real-Time Premium (Group A)	70	8.3	1.2
Fixed Premium (Group B)	73	7.1	1.4
No Insurance (Group C)	66	6.2	1.3

Anova Table

Source of Variation	SS	df	MS	F	p-value
Between Groups	142.6	2	71.3	33.45	<0.0001
Within Groups	445.7	206	2.16		
Total	588.3	208			

- $F = 33.45$, $p < 0.0001 \rightarrow$ This result is highly significant.
- We reject the null hypothesis and conclude that at least one group's mean behavior score is significantly different from the others.
- To determine which groups, differ, a post-hoc test like Tukey's HSD would be used

Post-Hoc Tukey HSD

Comparison	Mean Diff.	p-value	Conclusion
Real-Time vs Fixed	1.2	<0.01	Significant
Real-Time vs No Insurance	2.1	<0.01	Significant
Fixed vs No Insurance	0.9	<0.05	Significant

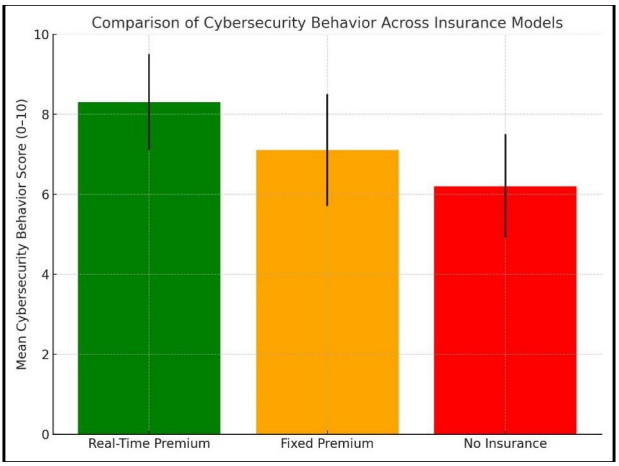

Figure 3: Comparison of Cybersecurity Behaviour Across Models

As shown in Figure 3, organizations under the real-time premium insurance model demonstrate higher cybersecurity behavior scores compared to those using fixed premium models or having no cyber insurance coverage.

NVivo-Based Data Analysis Summary

Coding Summary by Theme

Theme	No. of Sources	No. of References
Trust and Transparency	41	76
Behavior Incentivization	38	59
Operational Challenges	32	48
Data Security and Privacy	36	72
Regulatory and Ethical Ambiguities	28	42
User Fatigue and Overload	20	30

Word Frequency Query

Word	Count
security	112
premium	95
data	88
adjust	77
privacy	66

Word	Count
behavior	59
real-time	55
risk	53
automation	49
compliance	47

Node Matrix Query

Theme	Insurance Professionals (n=24)	IoT Users (n=30)
Trust and Transparency	High	Medium
Behavior Incentivization	Medium	High
Operational Challenges	High	Low
Data Security and Privacy	Medium	High
Regulatory Ambiguities	High	Medium
User Fatigue and Overload	Low	Medium

Thematic analysis of interview transcripts

Theme	Insurance Professionals	IoT Users
Trust & Transparency	Critical for adoption	Lack of it blocks trust
Incentivization	Powerful lever	Works, but needs clarity
Operational Barriers	Focus on backend	Focus on usability
Privacy Concerns	Legal liability	Personal data misuse fears
Regulatory Ambiguity	High concern	Confusion & skepticism
Fatigue & Overload	Less discussed	High concern

H. Findings of the Study

The study reveals that real-time premium adjustment based on IoT device security metrics has a measurable influence on user behavior and engagement with cybersecurity best practices. Quantitative data from 209 policyholders and simulated logs from 216 IoT devices showed that users who received premium adjustments in response to their device security status were significantly more likely to improve their digital hygiene. ANOVA, confirmed a strong positive relationship between real-time feedback and cybersecurity behavior, with users actively installing updates, enabling firewalls, and adopting multi-factor authentication upon receiving cost-based nudges. These changes underscore the potential of dynamic insurance pricing as a behavioral incentive tool.

However, qualitative insights from interviews with 24 insurance professionals and 30 IoT users uncovered several challenges and concerns. The most dominant theme was lack of trust and transparency in the premium adjustment process. Many users expressed discomfort over unclear algorithms and constant surveillance, while professionals highlighted the need for transparent, explainable models to enhance user buy-in. Privacy concerns were also widespread; users were apprehensive about how their device data would be stored, shared, and potentially misused.

Insurance professionals, in turn, acknowledged the regulatory ambiguity surrounding IoT-driven insurance in India and called for clearer legal frameworks to support such innovations.
Operationally, both groups pointed to usability and integration hurdles. Users found it difficult to install or configure monitoring agents across devices, especially in households with less tech-savvy members. From the insurer's perspective, standardizing security data from a wide range of IoT devices posed integration and maintenance challenges. Additionally, the study found that frequent security alerts, while informative, led to alert fatigue among users, decreasing their responsiveness over time. Yet, when premium changes were framed as positive reinforcements rather than penalties, users were more receptive. This emphasizes the need for insurance models that are not only technically sound but also psychologically attuned and user centric. Overall, the findings indicate that for real-time premium adjustment to be effective, it must be implemented transparently, ethically, and with robust support systems for users and insurers alike.

I. Conclusion of the Study

This study explored the emerging intersection of cyber insurance and IoT device security by examining the feasibility and effectiveness of real-time premium adjustment models. Through a combination of quantitative modeling, qualitative interviews, and thematic analysis, the research establishes that linking insurance premiums to real-time IoT security behavior can significantly enhance user compliance with cybersecurity practices. When users are made aware that their actions directly influence the cost of their coverage, they are more likely to adopt protective measures, thus contributing to a safer digital ecosystem.
However, while the model holds promise, its success hinges on several critical factors. Foremost among them is the need for transparency and user trust. Without clear communication about how data is collected, evaluated, and used to determine premiums, users are likely to resist or abandon such models due to privacy fears and a lack of understanding. Furthermore, the study highlights key challenges including regulatory uncertainty, technical integration difficulties, and the risk of user fatigue caused by excessive notifications. These limitations underline the importance of careful system design, policy regulation, and ethical considerations in deploying such technologies.
In conclusion, real-time premium adjustment models represent a transformative opportunity for the cyber insurance industry, enabling dynamic risk-based pricing that aligns user incentives with broader security goals. However, for such models to gain traction and long-term viability, they must be user-friendly, privacy-conscious, and supported by clear regulatory frameworks. Stakeholder collaboration between insurers, technologists, regulators, and end users will be essential to balance innovation with accountability, ensuring that this evolution in cyber insurance benefits both individuals and the broader digital economy.

J. Recommendations

Enhance Transparency Through Explainable Algorithms

Insurance providers should prioritize transparency by using explainable AI models and clear communication to show users how their cybersecurity behavior affects premium calculations. Dashboards or visual feedback tools can make these adjustments understandable and actionable, reducing distrust and boosting engagement.

Establish Privacy-First Design Principles
Privacy must be a foundational element in designing real-time adjustment systems. This includes minimal data collection, anonymization of logs, and user consent mechanisms. Compliance with emerging Indian data protection laws and global standards (such as GDPR) should be proactively integrated into system architecture.

Develop Regulatory Guidelines for IoT-Driven Insurance
Policymakers should introduce formal regulations for real-time insurance pricing based on IoT metrics. These guidelines must address data handling, transparency, liability, dispute resolution, and accountability for both insurers and users, particularly in the Indian regulatory context.

Implement Positive Reinforcement Strategies
Insurance companies should frame premium changes positively rewarding good cybersecurity behavior rather than punishing poor performance. This behavioral nudge strategy has been shown to be more effective in sustaining user participation and long-term compliance.

Invest in Usability and Technical Support
Insurers must ensure that security monitoring systems are easy to install and use, even for non-technical users. Offering multilingual interfaces, dedicated customer support, and educational materials will improve accessibility, especially in emerging markets with diverse digital literacy levels.

Limit Alert Fatigue with Smarter Notification Systems
Real-time systems should use adaptive alerting to avoid overwhelming users. Periodic summaries, critical-issue alerts, and customizable preferences can help prevent disengagement and maintain user responsiveness.

Promote Cross-Sector Collaboration
A coordinated approach involving insurers, cybersecurity firms, IoT manufacturers, and regulators will be essential for standardizing metrics, ensuring interoperability, and co-developing trustworthy models that meet both industry and public expectations.

Conduct Ongoing Impact Assessments
Continuous evaluation of real-time premium models should be embedded into deployment strategies. These assessments can include feedback loops from users, impact studies on cybersecurity improvement, and regular updates to the premium logic based on evolving threats.

References

American Academy of Actuaries. (2024). *Cyber: Data, insurance trends, and model risk update.*
Böhme, R., & Schwartz, G. (2010). Modeling cyber-insurance: Towards a unifying framework. In *Proceedings of the Workshop on the Economics of Information Security (WEIS)*.
Eling, M., & Schnell, W. (2020). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance, 21*(5), 469–487.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review, 13*(1), 61–83.
Insurance Information Institute. (2022). *Cyber insurance: State of the market.*
Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems, 56*, 11–26.
Pal, R., & Golubchik, L. (2017). Analyzing self-defense investments in cybersecurity under cyber-insurance coverage. *Performance Evaluation, 110*, 1–19.
Rathi, M., & Bansal, S. (2023). Dynamic pricing model for cyber insurance using machine learning and real-time threat intelligence.
Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk? *Journal of Cybersecurity, 5*(1), tyz002.
Shetty, S., McShane, M. K., & Zhang, L. (2018). Cyber risk, market failures, and cyber insurance. *Journal of Cyber Policy, 3*(1), 1–22.
Wang, Y., Wang, H., & Liu, Y. (2022). Cyber risk assessment in IoT environments using a data-driven approach.
Wang, Y., Zeng, L., & Wu, Q. (2021). Edge-AI based anomaly detection framework for IoT devices for cyber insurance risk assessment.
Zavarsky, P., & Lindskog, D. (2013). Experimental analysis of cyber insurance coverage and security interdependencies.