iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

DYNAMIC THIRD-PARTY CYBER RISK: DEVELOPING CONTINUOUS RISK ASSESSMENT MODELS FOR INTERCONNECTED DIGITAL SUPPLY CHAINS

Mojisola Ologe
Coauthor: Aisha Abdullahi

ABSTRACT
As organizations more and more have connected digital value chains, new cyber risks emerge not just from direct suppliers but also from software dependencies, third-party access privileges and common technology suppliers. Traditional Cyber Risk Management (CYRM) methods that take place on an annual basis and rely on individual vendors' evaluations might not account for the continuously evolving nature of cyber exposure, indirect exposures, or the lack of evidence. To overcome these limitations, this study suggests a model called Continuous Third Party Cyber Risk Assessment Model (CTCRAM). The model incorporates time-dependent supplier information, software dependencies, access privileges, threat intelligence and security controls as temporal dependencies in a temporal dependency network. It integrates probabilistic risk assessment, potential organisational losses, evidence uncertainty and risk propagation to enable ongoing risk reassessment and informed risk mitigation decisions. A design science approach is used to present a framework for evaluating the proposed model in comparison to static, periodic, and non-network-aware evaluation approaches. The criteria for evaluation are: reassessment latency, accuracy of risk estimation, calibration, quality of prioritization, robustness and utility in decision making. The proposed approach is designed to enable organisations to more effectively identify material changes in their exposure to third parties, be able to trace risks through interdependent exposures and better prioritise interventions within cybersecurity. But the utility of it will depend on data quality, model validation, and the improvement shown over existing approaches. This study proposes a structured framework for the third-party cyber risk management to be more responsive and defensible in a networked context of uncertainty because it combines dynamic evidence, network relationships and uncertainty in one assessment framework.

Keywords:
Third-party cyber risk, continuous risk assessment, digital supply chains, dependency networks, risk propagation, cybersecurity risk management.

I. INTRODUCTION

1.1 Background to the Study
More and more businesses rely on a web of vendors, cloud service providers, software developers, and other technology partners to provide critical services. While these connections can lead to greater efficiency, innovation, and the ability to access specialized expertise, they also create a cybersecurity dependency that is outside of an organization's direct control. Multiple organizations are vulnerable when software components are vulnerable, suppliers are compromised, or there are too many privileges granted to third parties. When a digital supply chain is more complex, evaluating the vendors individually may only address a portion of the organization's risk because risks can pass from one vendor to another via interconnected systems and relationships (Boyson, 2014; NIST, 2022a).

Traditional third party cyber risk management is founded on a combination of questionnaires, audits, certifications and third party ratings that are carried out periodically. These are useful for setting a baseline level of security; however they lack the ability to reflect the rapidly changing vulnerabilities, access privileges, supplier situation, and threat exposure. Moreover, information is often spread out in procurement systems, access-management platforms, software bills of materials and threat-intelligence feeds. While supply chain risk management is one of the established frameworks, a challenge is how to combine the varying and sometimes uncertain signals into a constant, evolving evaluation of cyber risk (NIST, 2024). The continuous assessment approach proposed in this study, therefore, features vendor conditions, software dependencies, access privileges, threat exposure and risk propagation, which enable the identification of threats in time, the decision-making of appropriate risk mitigation measures, and improved prioritization of cybersecurity investments.

1.2 Statement of the Research Problem
Though business is increasingly aware of third-party cyber risk, they do not have the ability to calculate the impact of third-party suppliers and technology changes on their cyber risk. They are typically based on periodic reviews,

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

static risk classifications and isolated vendor assessments, which are ineffective in detecting new vulnerabilities, changing access rights and new threats (Cheimonidis & Rantos, 2023). Interconnected digital supply chains also bring indirect and common exposures, compromises can impact number of organizations, causing significant financial impact (Crosignani et al., 2023). High risks associated with unknown and incomplete information regarding suppliers, subcontractors, software requirements and security measures. Therefore, the more frequent the assessments, the more the results are unreliable without consideration of dependency relationships, evidence reliability, and the possibility of double counting shared exposures. This research tries to overcome this limitation by proposing a network-aware and dynamically evolving cyber risk assessment model that integrates temporal updates, uncertainty, risk propagation, and potential losses to third parties.

1.3 Aim and Objectives of the Study

The aim of this study is to develop and evaluate a continuous third-party cyber risk assessment model that estimates how changes in vendors, software dependencies, access privileges, and threat exposure affect organizational cyber risk across an interconnected digital supply chain.

The specific objectives are to:

1) Examine existing third-party cyber risk assessment approaches and identify their limitations in addressing temporal change, interdependence, and uncertainty.
2) Develop a dynamic representation of the relationships among organizations, vendors, software components, access pathways, and critical business assets.
3) Formulate a risk estimation model that updates incident likelihood and potential organizational loss as new evidence becomes available.
4) Establish mechanisms for incorporating dependency-based risk propagation, shared exposure, and uncertainty into organizational risk estimates.
5) Evaluate the proposed model against static, periodic, and non-network-aware assessment approaches using appropriate performance and robustness measures.
6) Determine how continuous risk estimates can support the prioritization of mitigation actions and cybersecurity investments.

These objectives distinguish model development from model evaluation. The study does not assume in advance that a continuous approach will outperform existing methods. Its effectiveness must be established through a transparent comparison using appropriate data, assumptions, and evaluation procedures.

1.4 Research Questions

The study is guided by the following research questions:

RQ1: What limitations in existing third-party cyber risk assessment approaches hinder their ability to reflect changes in interconnected digital supply chains?

RQ2: How can changes in vendor security conditions, software dependencies, access privileges, and threat exposure be incorporated into a continuously updated cyber risk model?

RQ3: To what extent does incorporating dependency relationships and risk propagation improve the estimation of organizational cyber risk compared with models that assess third parties independently?

RQ4: How can uncertainty and incomplete information be represented so that risk estimates remain interpretable and useful for decision-making?

RQ5: How effectively does the proposed model identify material changes in risk and prioritize mitigation actions compared with static and periodic assessment baselines?

Together, these questions address the problem, the proposed analytical approach, and its evaluation. They also provide a basis for aligning the literature review, mathematical formulation, experimental design, and discussion of findings.

1.5 Significance of the Study

The study has four main areas of significance. Theoretically, it conceptualizes third-party cyber risk as a dynamic property of interconnected systems, integrating supply chain risk management, network analysis, probabilistic reasoning, and continuous assessment. Methodologically, it proposes a reproducible approach for updating risk estimates as new evidence emerges, accounting for likelihood, potential loss, uncertainty, and risk prioritization, with comparative evaluation against simpler methods.

Practically and in governance, the proposed model could help cybersecurity and enterprise risk managers identify emerging supplier risks, trace vulnerabilities through dependent applications and business services, and prioritize mitigation measures. It could also strengthen coordination among cybersecurity, procurement, IT, and enterprise risk functions, supporting NIST's emphasis on integrating supply chain security into organizational risk management (Boyens et al., 2022). However, the model's value must be demonstrated through measurable

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

improvements in estimation accuracy, detection speed, prioritization, or mitigation decisions rather than assumed from more frequent monitoring alone.

1.6 Scope and Delimitations of the Study

The study focuses on organizational cybersecurity risks arising from external vendors, third-party technology providers, software components, and associated access relationships within interconnected digital supply chains. Four categories of change are central to the proposed model:

- Vendor conditions: changes in security posture, reported incidents, assurance evidence, and relevant control weaknesses.
- Software dependencies: newly disclosed vulnerabilities, component updates, dependency relationships, and the extent to which affected components support critical applications.
- Access privileges: changes in third-party permissions, privileged accounts, connectivity, and access to sensitive systems or data.
- Threat exposure: changes in threat intelligence, exploit availability, observed attack activity, and other evidence relevant to the likelihood of a cyber incident.

The model will consider both direct and indirect exposure, including shared dependencies and possible risk propagation between connected entities. It will also distinguish estimated risk from the confidence that can reasonably be placed in available evidence.

The research will focus on model development and comparative evaluation rather than on creating a universal platform for every cybersecurity environment. The specific data strategy—historical incident data, public vulnerability and dependency data, simulated scenarios, or a hybrid approach—must be established in the methodology. Where simulated data are used, conclusions will be limited to the assumptions and scenarios represented; simulation results alone cannot demonstrate effectiveness in operational environments.

The study will not assume that every vulnerability leads to an incident, that every supplier relationship creates equal exposure, or that all risks can be expressed reliably as a single score. The proposed model will instead seek to estimate risk in relation to organizational assets, threat scenarios, dependencies, and potential consequences.

1.7 Definition of Key Terms

For consistency, the following terms are used throughout the study.

Term	Operational definition
Third-party cyber risk	The potential for a cyber incident involving an external supplier, service provider, software component, or access relationship to cause harm to the focal organization.
Continuous risk assessment	The repeated or event-triggered updating of risk estimates as relevant evidence or system conditions change. It does not necessarily require every data source to be monitored in real time.
Digital supply chain	The interconnected network of organizations, services, software components, and technology relationships involved in developing, delivering, operating, or supporting digital products and services.
Risk propagation	The transmission or amplification of potential cyber consequences through dependencies or relationships connecting supply chain entities.
Dependency relationship	A technical or operational connection through which an organization, application, or business service relies on another entity or component.
Risk exposure	The extent to which an organization may be affected by a specified threat scenario, considering relevant vulnerabilities, access pathways, dependencies, and business consequences.
Epistemic uncertainty	Uncertainty arising from incomplete knowledge, limited observations, uncertain parameters, or imperfect models.
Expected cyber loss	The probability-weighted estimate of loss associated with defined cyber incident scenarios over a specified period.
Risk confidence	An indication of the strength, completeness, timeliness, and reliability of the evidence supporting a risk estimate.
Mitigation decision	An action intended to reduce incident likelihood, limit consequences, improve resilience, or otherwise manage identified cyber risk.

These definitions establish the conceptual boundaries of the study. In particular, continuous assessment is understood as a disciplined process of updating risk estimates—not simply the frequent collection of security alerts.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

II. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Conceptual Review of Third-Party Cyber Risk

Third-party cyber risk arises when an organization's dependence on external entities creates pathways through which cybersecurity incidents can affect its systems, information, operations, or financial position. Such risks may result from inadequate supplier security controls, compromised service providers, vulnerable software components, insecure connections, or poorly managed third-party access. Unlike risks originating within internal infrastructure, third-party cyber risk is partly shaped by conditions beyond an organization's direct control. Consequently, even organizations with strong internal security may remain exposed through vendors with privileged access or widely used software dependencies.

Cyber supply chain risk management emphasizes the strategic importance of identifying and managing these external dependencies (Boyson, 2014; Boyens et al., 2022). However, identifying vulnerabilities does not automatically establish their organizational significance. Actual risk depends on factors such as exploitability, software usage, access privileges, business criticality, and potential losses. Third-party cyber risk is therefore a contextual construct shaped by the interaction between threats, vulnerabilities, exposure pathways, and consequences. Supplier security ratings can provide useful indicators, but they may not adequately reflect an organization's specific dependencies, access arrangements, or operational exposure.

2.2 Static and Periodic Risk Assessment Approaches

Traditional approaches to cyber risk assessment generally combine asset identification, threat and vulnerability analysis, control evaluation, likelihood estimation, and impact assessment. In third-party management, these principles are commonly implemented through vendor questionnaires, security audits, contractual requirements, certifications, external ratings, and periodic reassessments. Their principal strength is governance: they help organizations establish minimum requirements, document supplier obligations, and maintain evidence of due diligence.

Nevertheless, periodic assessment can create a gap between the time a risk changes and the time that change is recognized. A vendor may be assessed in January, experience a significant compromise in March, and remain classified as low risk until its next scheduled review. The classification may have been reasonable when assigned but no longer reflect the available evidence.

Static models also tend to compress several dimensions into one rating. Two suppliers assigned the same risk category may differ considerably in their access privileges, substitutability, software dependencies, and potential impact on business operations. The shared rating can conceal these differences. These limitations do not make periodic assessment unnecessary. Instead, they suggest that periodic reviews should establish a governance baseline, while material changes in exposure should trigger additional assessment. Continuous assessment can complement established risk management practices rather than replace contractual oversight, audits, or human judgment.

2.3 Dynamic Cyber Risk Assessment

Dynamic cyber risk assessment updates risk estimates as new observations become available. These observations may include newly disclosed vulnerabilities, changes in asset criticality, threat intelligence, security incidents, configuration changes, or modifications to access permissions.

Cheimonidis and Rantos (2023) review dynamic risk assessment methods and discuss approaches that use Bayesian networks, hidden Markov models, and other analytical techniques to represent changing cyber conditions. Their review illustrates that dynamic assessment is not a single algorithm but a family of methods for updating risk as the environment evolves.

Bayesian methods are particularly relevant when evidence arrives incrementally. Suppose a supplier was initially assessed using a questionnaire and later becomes associated with an actively exploited vulnerability. The new evidence can update the estimated probability of a defined incident. The magnitude of that update should depend on the relevance of the vulnerability to the organization's environment, the presence of effective controls, and the reliability of the information.

A dynamic model must also distinguish between the occurrence of a new observation and a genuine change in underlying risk. A new threat-intelligence report may provide information about a previously existing threat rather than indicate that the threat itself has newly emerged. Similarly, the discovery of a vulnerability can increase estimated exposure without proving that an incident will occur.

The central methodological implication is that the model should update its estimates in response to evidence while preserving a clear distinction between observed facts, inferred conditions, and uncertain assumptions.

2.4 Software Dependencies and Supply Chain Visibility

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Modern applications frequently incorporate externally developed libraries, packages, frameworks, and services. This reduces development effort but creates dependencies that may not be immediately visible to the organization using the software.

A software bill of materials (SBOM) provides a structured inventory of software components and their relationships. It can support vulnerability identification by helping organizations determine whether an affected component is present in their applications. NIST's software supply chain guidance discusses the role of SBOMs, vulnerability information, and contextualized dependency data in improving supply chain visibility (NIST, 2022b).

However, an SBOM is an inventory, not a complete risk assessment. A listed vulnerability may affect a component that is not deployed, is unreachable, or is protected by compensating controls. Conversely, incomplete or outdated component records can create false confidence by making an application's dependency structure appear more complete than it is.

Research by Reichert and Obelheiro (2024) identifies gaps in the software supply chain security literature, including limited attention to some cloud-related dependencies and shortcomings in threat modelling and validation. Xia et al. (2023) likewise examine practitioner experience with SBOMs, highlighting challenges associated with their practical adoption. These findings support the integration of dependency inventories with vulnerability intelligence, asset criticality, supplier information, and organizational context. In the proposed model, software dependencies are represented as relationships in a changing network rather than as isolated inventory records.

2.5 Interdependence and Risk Propagation

A digital supply chain is not simply a list of vendors. It is a network of relationships through which services, data, software, privileges, and operational dependencies connect organizations and technology components.

Network-based modelling provides a way to represent these relationships. Graph theory distinguishes between nodes, which represent entities, and edges, which represent relationships between them. This representation makes it possible to examine direct exposure, indirect dependencies, highly connected components, and concentration risk (Newman, 2018).

The relevance of network structure is not merely theoretical. Crosignani et al. (2023), examining cyberattack transmission through firms' supply chains, found that cyberattack consequences extended from directly affected firms to connected customers and that the economic effects could be amplified across these relationships.

The implication for cyber risk assessment is that a supplier's importance depends partly on its position in the network. A vulnerability affecting a small, replaceable supplier may have limited consequences. The same vulnerability affecting a shared identity provider, cloud service, or critical software component could create substantial exposure across several business functions.

Yet network connectivity alone does not determine risk. A highly connected component may be protected by strong controls, while a poorly connected supplier with privileged access to a critical system may present substantial exposure. Consequently, network position should inform risk estimation without becoming a substitute for vulnerability, threat, access, and impact analysis.

A further challenge is correlated risk. If several business services depend on the same supplier, their losses may occur together rather than independently. Adding individual expected losses without accounting for shared causes can distort aggregate estimates. A sound model must represent common dependencies explicitly and avoid counting the same incident repeatedly.

2.6 Uncertainty in Cyber Risk Estimation

Cyber risk estimates are rarely based on complete information. Organizations may not know the exact frequency of successful attacks against a supplier, the full extent of its subcontracting arrangements, or the effectiveness of its internal security controls. Consequently, numerical precision should not be confused with certainty.

Four forms of uncertainty are relevant:

1. **Aleatory uncertainty:** inherent variability in events, such as the timing or occurrence of an attack.
2. **Epistemic uncertainty:** limited knowledge about a supplier's actual security condition or the likelihood of exploitation.
3. **Measurement uncertainty:** errors, omissions, or delays in vulnerability records, questionnaires, logs, and other observations.
4. **Structural uncertainty:** uncertainty about whether the model adequately represents the relationships and mechanisms that generate risk.

These distinctions matter because different uncertainties require different responses. More frequent observations may reduce some measurement uncertainty, but they will not necessarily resolve a poorly specified causal model.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Similarly, obtaining an additional supplier questionnaire may improve visibility while leaving the likelihood of a sophisticated attack uncertain.

Bayesian inference provides a formal basis for updating beliefs as new evidence becomes available (Pearl, 1988; Koller & Friedman, 2009). Monte Carlo simulation can complement this approach by representing uncertainty in model parameters and estimating a distribution of potential losses rather than a single deterministic figure (Vose, 2008).

The proposed model therefore treats risk estimates as conditional on the available evidence. It also recommends recording evidence quality separately from the estimated risk itself. A low estimate supported by incomplete information should not automatically receive the same management response as a low estimate supported by current, reliable, and corroborated evidence.

2.7 Theoretical and Analytical Foundations

The study combines four complementary foundations. They serve different purposes and should not be treated as interchangeable theories.

Systems theory: Systems theory emphasizes that an organization's outcomes depend on interactions among connected components, not merely on the characteristics of individual components. In this study, it provides the conceptual basis for examining cyber risk across the wider supply chain rather than restricting analysis to isolated vendors.

Graph theory and network science: Graph theory provides the representation needed to map supplier relationships, software dependencies, access pathways, and shared services. Network analysis supports the identification of critical nodes, indirect exposure, and concentration points (Newman, 2018).

Bayesian inference: Bayesian reasoning supports the updating of incident probabilities as new evidence arrives. It is especially relevant where observations are incomplete or differ in reliability (Pearl, 1988; Koller & Friedman, 2009).

Decision theory: Decision theory connects risk estimates to organizational choices. A model is useful not merely because it produces a probability or loss estimate, but because it helps decision-makers compare mitigation options under budget, operational, and risk-tolerance constraints.

These foundations are supported by established risk management standards. The proposed contribution, therefore, lies in integrating these foundations into a single operational workflow for continuous third-party cyber risk estimation. The novelty claim is therefore a proposed integration and evaluation contribution, not an assertion that dynamic risk assessment, Bayesian inference, or network analysis is individually new.

2.8 Empirical Review and Research Gap

The literature establishes several important points. First, supply chain cyber incidents can create consequences beyond the initially compromised organization (Crosignani et al., 2023). Second, dynamic assessment methods can incorporate changing evidence into risk estimation (Cheimonidis & Rantos, 2023). Third, software component inventories can improve visibility into dependency-related exposure, although practical adoption and data quality remain important concerns (Xia et al., 2023; Reichert & Obelheiro, 2024). However, these strands of research do not, by themselves, provide a complete operational answer to the research problem. An inventory can identify affected components without quantifying organizational loss. A dynamic risk model can update probabilities without adequately representing supplier concentration. A network model can identify dependencies without determining whether an incident is plausible or financially consequential.

The study therefore addresses four connected gaps:

- Temporal gap: the need to specify when and how new evidence changes risk estimates.
- Dependency gap: the need to connect vendor, software, access, and business-service relationships within a unified representation.
- Uncertainty gap: the need to distinguish estimated risk from confidence in the evidence and model assumptions.
- Decision gap: the need to translate changing risk estimates into transparent, cost-conscious mitigation priorities.

These gaps motivate a model that combines event-triggered updating, network-aware exposure analysis, probabilistic loss estimation, and mitigation decision support. Its value must be tested against simpler alternatives rather than inferred from its complexity.

2.9 Conceptual Framework

The conceptual framework consists of five linked stages:

1. Change detection: identify new or modified vendor conditions, vulnerabilities, access privileges, and threat indicators.
2. Evidence assessment: establish the relevance, reliability, completeness, and timeliness of observations.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

3. Dynamic risk inference: update the estimated probability of defined cyber incident scenarios.
4. Dependency and loss analysis: trace plausible exposure through connected entities and estimate organizational consequences while accounting for common causes.
5. Decision and feedback: prioritize mitigation, record decisions, and update the model as controls or relationships change.

The framework treats risk assessment as a feedback process. Mitigation can alter access, reduce exposure, improve recovery capability, or change dependency relationships. Those changes should be reflected in subsequent estimates.

The principal conceptual relationship is that organizational cyber risk depends on the evolving condition of external entities, the structure of their dependencies, the quality of available evidence, and the organization's ability to prevent or absorb potential losses.

III. RESEARCH METHODOLOGY

3.1 Research Design

The study adopts a design science research approach supported by quantitative model evaluation. Design science is appropriate because the central objective is to develop an analytical artefact—a continuous third-party cyber risk assessment model—and evaluate its performance against defined requirements (Hevner et al., 2004; Peffers et al., 2007).

The research proceeded through six activities: problem identification, definition of model requirements, design of the assessment framework, implementation of the model, comparative evaluation, and communication of the findings. The study is not designed to establish that every organization will benefit equally from continuous assessment. Instead, it will test whether the proposed model provides measurable improvements under clearly specified conditions.

3.2 Research Questions and Evaluation Propositions

The research questions guide both model development and testing. The following propositions are evaluated where suitable data are available:

- P1: Event-triggered assessment will reduce the delay between a material risk change and its recognition compared with periodic assessment.
- P2: A network-aware model will estimate indirect exposure more comprehensively than a model that assesses third parties independently.
- P3: Incorporating evidence quality and uncertainty will improve the interpretability and calibration of risk estimates when compared with approaches that treat all inputs as equally reliable.
- P4: A model that combines dynamic risk estimation with mitigation costs will produce more defensible intervention priorities than one based solely on unadjusted risk scores.

These are propositions to be tested, not established findings. Their evaluation will depend on the availability of appropriate reference data and the design of the comparison experiments.

3.3 Data Sources and Collection Strategy

The model requires evidence about entities, relationships, changing security conditions, incident scenarios, and potential consequences. A hybrid data strategy is proposed, subject to access and feasibility.

Data category	Potential sources	Purpose
Vendor and relationship data	Supplier registers, procurement records, contractual records	Identify third parties and business dependencies
Software dependency data	SBOMs, package manifests, dependency repositories	Identify software components and downstream applications
Vulnerability information	National Vulnerability Database, Common Vulnerabilities and Exposures records	Identify known vulnerabilities and relevant severity information
Threat evidence	Public threat advisories, exploitation reports, security alerts	Update the plausibility of defined incident scenarios
Access information	Identity and access management records, privileged access logs	Assess the scope and sensitivity of third-party access
Incident and loss information	Authorized historical incident records, public incident reports, documented case studies	Inform probability and consequence estimation
Mitigation information	Security control records, remediation estimates, recovery plans	Estimate intervention costs and potential risk reduction

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

The National Vulnerability Database and CVE records can provide useful vulnerability information, but neither source independently establishes whether a particular vulnerability is exploitable in a specific organizational environment. Contextual information is necessary to determine relevance. The preferred design is to combine real or public observations with controlled scenarios where the available incident data are insufficient. The analysis must clearly distinguish observed data from synthetic inputs. Synthetic scenarios can test model behaviour under known conditions, but they cannot independently establish real-world predictive accuracy.

3.4 Unit of Analysis and Population

The principal unit of analysis is a third-party-related cyber incident scenario within a defined organizational dependency network over a specified time horizon.

A scenario may involve a compromised vendor account, exploitation of a vulnerable software component, compromise of a cloud service, or a security incident affecting a shared provider. Each scenario should be connected to the entities and business services through which its consequences could reach the focal organization.

The population of interest consists of organizational digital supply chains with external technology or service dependencies. The actual evaluation sample will depend on the accessible dataset. If the research uses a simulated network, the sample will consist of generated nodes, relationships, events, and scenarios rather than a representative sample of real organizations.

This distinction is essential when interpreting results. Performance on a simulated network may demonstrate computational feasibility and internal consistency, but broader claims about organizational effectiveness require external validation.

3.5 Variable Specification

The proposed model will use the following principal variables.

Variable	Description	Measurement approach
$P_{s(t)}$	Estimated probability of incident scenario *s* over a defined horizon at time *t*	Historical estimates, probabilistic inference, or calibrated scenario assumptions
$L_{s(t)}$	Organizational loss associated with scenario *s* at time *t*	Financial and operational consequence estimates
D(t)	Dependency network at time *t*	Nodes, directed edges, edge types, and criticality attributes
$A_{j(t)}$	Access privileges associated with entity or account *j*	Permission scope, privilege level, and asset sensitivity
$V_{j(t)}$	Relevant vulnerability state for entity or component *j*	Vulnerability presence, applicability, exploitability, and mitigation status
$T_{s(t)}$	Threat evidence relevant to scenario *s*	Exploitation evidence, threat reports, and contextual indicators
$Q_{j(t)}$	Quality of evidence concerning entity or component *j*	Completeness, timeliness, provenance, and corroboration
$C_{a(t)}$	Cost of mitigation action *a*	Direct implementation and relevant operating costs
R(t)	Aggregate organizational cyber risk over the defined horizon	Probability-weighted loss distribution and related measures

Variables will be operationalized before evaluation. The study must avoid double-counting correlated indicators, such as a vulnerability severity score and a risk rating that already incorporates that same severity.

3.6 Proposed Model Specification

The model begins by defining a set of cyber incident scenarios *S*. Each scenario represents a plausible event with a specified initiating condition, affected assets, potential propagation pathways, and organizational consequences. The baseline expected loss at time t is expressed as:

$$E[L_t \mid D_t] = \sum_{s=1}^{s} P(S_s \mid D_t) L_s(t)$$

where:

- $E[L_t \mid D_t]$: Expected organizational loss at time t.
- S_s: Incident scenario s.
- $P(S_s \mid D_t)$ is the probability of the scenario given available evidence;
- $L_s(t)$ is the potential organizational loss associated with the scenario;
- $D_t$is the evidence available at time *t*.

This formulation is a starting point, not the complete model. It assumes that scenario probabilities and losses are estimated consistently and that overlapping scenarios are handled appropriately. If scenarios are mutually

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

exclusive, their probabilities can be combined directly in the expected-loss calculation. If scenarios overlap or share initiating events, the model must represent their joint dependence to avoid double-counting.

For each scenario, probability estimation will consider relevant threat evidence, vulnerability applicability, access conditions, existing controls, and dependency structure. The model will not assume that a vulnerability score directly equals an incident probability. Instead, such scores may serve as evidence within a broader estimation process.

A simplified representation is:

$$P(S_s \mid D_t) = f(T_s(t), V_s(t), A_s(t), D(t), C_s(t), Q_s(t))$$

where $C_s(t)$ denotes the relevant security-control state and $f(\cdot)$ represents a probabilistic inference procedure to be specified and calibrated during implementation.

This expression identifies the model inputs but does not establish a functional form. The final implementation may use a Bayesian network, a dynamic Bayesian network, or another method justified by the data and evaluation requirements.

3.7 Dependency Modelling and Risk Propagation

The digital supply chain will be represented as a directed, typed graph:

$$G_t = (V_t, E_t)$$

where V_t represents vendors, software components, access identities, organizational assets, and business services, while E_t represents relationships such as service provision, software inclusion, privileged access, or operational dependence.

The graph is time-dependent because suppliers can be added or removed, software components can change, and access permissions can be granted or revoked.

Risk propagation will be modelled through plausible causal or dependency pathways. For example, a vulnerable component may affect an application that supports a business service, which in turn affects an organizational process. The existence of a path establishes potential exposure, not certainty that an attack will propagate along it.

The model will distinguish between:

- direct exposure to a supplier or component;
- indirect exposure through dependent entities;
- common-cause exposure involving shared providers or components;
- concentration risk arising from reliance on a limited number of critical providers.

Propagation probabilities will require defensible assumptions or empirical calibration. Where evidence is insufficient, the model should present scenario ranges or sensitivity analyses rather than assign unjustified precision to every edge.

3.8 Event-Triggered Updating

The proposed model will update risk estimates when material changes are detected. Relevant triggers include newly disclosed vulnerabilities affecting deployed components, confirmed supplier incidents, changes to privileged access, significant alterations to dependency relationships, and credible evidence of active exploitation.

Each event will pass through a validation process before influencing the risk estimate. The process will record the source, observation time, event time where known, confidence, relevance, and affected entities.

The model will distinguish three timestamps:

1. Event time: when the underlying condition is believed to have changed.
2. Observation time: when the organization receives or records the evidence.
3. Assessment time: when the model incorporates the evidence into its risk estimate.

This distinction supports measurement of reassessment latency and helps prevent temporal leakage during evaluation. Where information arrives late, the model should not retrospectively behave as though the organization knew it earlier.

A scheduled reassessment may still be necessary for information that changes gradually or is not observable through automated feeds. Continuous assessment is therefore defined operationally as a combination of event-triggered updates and periodic data-quality checks, not as an assumption that every relevant condition is observable in real time.

3.9 Uncertainty and Evidence Quality

The model will represent uncertainty in both scenario probabilities and loss estimates. Where possible, probability distributions or intervals will be used instead of unsupported point estimates.

Evidence quality will be tracked separately from estimated risk. It may be represented through a structured set of attributes, including source reliability, data completeness, recency, and corroboration. These attributes should influence inference only through a justified method; an arbitrary quality multiplier could distort the result.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Where evidence is incomplete, the model will identify the missing information and evaluate alternative assumptions. Sensitivity analysis will determine whether the recommended action changes under plausible variations in the unknown parameters.

This approach is particularly important when assessing small suppliers or opaque subcontracting arrangements. A lack of public information should not automatically be interpreted as evidence of poor security, but neither should it be treated as proof of safety.

3.10 Mitigation Prioritization

Risk estimates will inform, but not automatically determine, mitigation decisions. Candidate interventions may include revoking unnecessary access, patching affected components, introducing compensating controls, requiring supplier remediation, segmenting systems, improving monitoring, or replacing a supplier.

Let a represent a candidate mitigation action and (C(a) its implementation cost. A simplified decision objective is:

$$a^* = \arg\min_{a \in A} [E[L \mid a, D_t] + C(a)]$$

where $\mathcal{A}$ is the set of feasible interventions. The model seeks to select an action that minimizes expected residual loss plus mitigation cost, subject to organizational constraints.

This formulation assumes that losses and mitigation costs can be expressed on a comparable basis. In practice, organizations may also impose mandatory controls, regulatory obligations, risk appetite limits, or minimum resilience requirements. Such constraints must be included rather than allowing the optimization procedure to recommend an inexpensive action that violates essential security obligations.

3.11 Comparative Evaluation Design

The proposed model will be evaluated against four approaches:

1. Static baseline: risk estimates remain fixed until a major scheduled review.
2. Periodic baseline: risk estimates are refreshed at predefined intervals using available evidence.
3. Dynamic non-network baseline: evidence is updated continuously or when events occur, but third-party dependencies are not explicitly modelled.
4. Full proposed model: dynamic updating, dependency-aware risk analysis, uncertainty handling, and mitigation prioritization are combined.

All approaches should use equivalent information wherever possible, the same evaluation horizon, and comparable scenario definitions. Otherwise, performance differences may reflect data advantages rather than the value of the modelling approach.

The evaluation will include ablation tests that remove network analysis, uncertainty handling, or event-triggered updating one at a time. These tests will help determine which components contribute measurable value.

3.12 Performance Metrics and Statistical Analysis

Evaluation metrics will be selected according to the type of outcome being assessed.

- Reassessment latency: time between the availability of material evidence and the corresponding risk update.
- Probability calibration: agreement between predicted probabilities and observed event frequencies, where sufficient observations exist.
- Brier score or log loss: appropriate measures of probabilistic prediction performance when reliable outcome labels are available.
- Expected-loss error: difference between estimated and observed or defensibly reconstructed losses, where comparable loss data exist.
- Risk-ranking quality: ability to place genuinely high-consequence scenarios or entities near the top of a priority list.
- Robustness: stability of results under missing data, delayed observations, parameter changes, and alternative network structures.
- Decision utility: comparison of residual expected loss and intervention costs under equivalent decision constraints.

No single metric will be treated as sufficient. For example, a model may rank suppliers effectively while producing poorly calibrated probabilities. Conversely, a model may have reasonable aggregate calibration but fail to identify a critical shared dependency.

For temporal evaluation, the study will use time-based holdout sets or rolling-origin evaluation where data permit. Information that became available after the prediction time must not be used to generate that prediction. Statistical uncertainty around performance differences should be reported, and results should be interpreted in relation to the number and quality of observed incidents.

3.13 Validity, Reliability, and Ethical Considerations

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Construct validity are supported by explicit definitions of risk, exposure, incident scenarios, and organizational loss. Internal validity will be strengthened by using controlled comparisons and documenting assumptions. External validity are assessed cautiously, particularly if the model is evaluated mainly with simulated data.
Reproducibility requires documentation of data sources, transformations, graph construction rules, parameter choices, scenario assumptions, and model versions. Where data cannot be shared, the study provided a sufficiently detailed description of the evaluation procedure for others to reproduce its logic using comparable data.
Ethical and operational safeguards are necessary. The research minimizes identifiable information, respects access permissions, and protects confidential data. Model outputs support accountable human decisions rather than automatically penalize suppliers on the basis of incomplete or unverified evidence.

3.14 Methodological Limitations

The principal limitations involve incomplete data, inconsistent vendor records, sparse incident observations, uncertain loss estimates, and limited visibility into fourth-party dependencies. These constraints affect both model calibration and the reliability of risk propagation estimates.
A hybrid dataset can improve scenario coverage, but synthetic data may not reproduce real-world attack behaviour or organizational responses. Similarly, a sophisticated model is computationally demanding and difficult to maintain if its data pipelines and assumptions are not well governed.
The study therefore evaluates the model's incremental value relative to simpler approaches. Complexity will be justified only where it produces demonstrable improvements in risk estimation, reassessment speed, robustness, or decision quality.

IV. PROPOSED CONTINUOUS THIRD-PARTY CYBER RISK ASSESSMENT MODEL

4.1 Model Architecture

The proposed model, referred to here as the Continuous Third-Party Cyber Risk Assessment Model (CTCRAM), comprises six functional layers:

1) Data ingestion: receives supplier records, software inventories, vulnerability information, threat intelligence, access records, and incident observations.
2) Entity and relationship resolution: identifies the relevant organizations, components, accounts, assets, and business services, including duplicate or inconsistent records.
3) Temporal dependency graph: represents the changing relationships among entities and records when each relationship was valid.
4) Risk inference engine: updates scenario probabilities and consequence estimates using current evidence and dependency information.
5) Decision-support layer: ranks exposures, compares mitigation actions, and identifies cases requiring further investigation.
6) Governance and feedback layer: records decisions, monitors data quality, and updates the model as controls and relationships change.

The layers are designed to separate observation from inference. A vulnerability scanner may identify a potential weakness, for example, but the inference engine must determine whether that weakness applies to a deployed component and how it affects organizational exposure.

4.2 Dynamic Risk Quantification

At each assessment time, the model estimates expected loss across the defined scenario set. The estimate changes when new evidence modifies the probability of an incident, the extent of exposure, the potential consequences, or the effectiveness of controls.
The basic relationship remains:

$$R(t) = \sum_{s=1}^{s} P(S_s \mid D_t) L_s(t)$$

This expression is appropriate when scenario losses can be aggregated without double-counting. Where scenarios overlap, the model should instead estimate a joint loss distribution or use a simulation that explicitly represents shared events and correlated consequences.
The model should also retain scenario-level estimates. A single aggregate number can conceal the fact that risk is concentrated in one critical provider or one software component. Reporting expected loss alongside the leading scenarios, uncertainty intervals, and key contributing dependencies provides a more useful basis for action.

4.3 Modelling Vendor, Software, Access, and Threat Changes

The model will incorporate four major change categories.
Vendor changes: New incident reports, changes in security assurance, ownership changes, and alterations in service criticality can trigger reassessment. Vendor-related observations should be linked to the services and assets that actually depend on the supplier.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Software changes: New vulnerabilities, package updates, component removals, and changes in dependency inventories can alter exposure. The model must establish whether an affected component is present and relevant before increasing the estimated risk of an incident.
Access changes: New privileged accounts, expanded permissions, new remote connections, and access revocation events can alter the potential pathways through which a supplier-related incident could affect the organization. Access scope and asset sensitivity should inform the estimated consequences.
Threat changes: Credible evidence of active exploitation or a significant change in threat activity may update scenario probabilities. However, the model must distinguish threat prevalence from environment-specific exploitability. A widely exploited vulnerability may still be irrelevant to a particular organization if the affected component is absent.
These event categories are inputs to the model, not independent risk multipliers. Their effects should be represented through the defined incident scenarios to avoid counting the same condition repeatedly.

4.4 Dependency-Based Risk Propagation

The temporal dependency graph supports the analysis of indirect exposure. For example, an organization may rely on a software vendor whose product incorporates a vulnerable open-source library. That product may support an application connected to a critical business service. The model traces the relationships to identify plausible pathways between the vulnerable component and the business consequence.
The propagation process should consider:

- whether a dependency is direct or indirect;
- whether the affected component is deployed and reachable;
- whether relevant controls interrupt the pathway;
- whether multiple services share the same dependency;
- whether losses across affected services are correlated;
- whether an alternative supplier or recovery option exists.

The model should not assume that risk propagates equally through every network edge. A contractual relationship does not necessarily create a technical attack path, and a technical dependency does not automatically imply that a compromise will cause a business interruption. Relationship types and their security implications must be defined explicitly.

4.5 Continuous Updating and Escalation

Each update should produce a record of the evidence received, affected entities, prior risk estimate, revised estimate, and reason for the change. This supports auditability and helps analysts distinguish material risk changes from routine fluctuations.
Escalation rules may be based on changes in expected loss, the emergence of a critical vulnerability, the discovery of a new privileged access pathway, or a decline in confidence due to missing or stale data. Thresholds should be defined by the organization according to its risk appetite and operational requirements rather than assumed to be universal.
Where evidence is ambiguous, the model should flag the issue for analyst review rather than generate an apparently precise conclusion. The purpose of continuous assessment is to improve the timing and quality of decisions, not to eliminate human judgment.

4.6 Model Outputs and Implementation Requirements

The model's outputs should include:

- current expected loss and, where feasible, uncertainty intervals;
- the leading incident scenarios and their contributing factors;
- critical suppliers and shared dependencies;
- material changes since the previous assessment;
- data-quality and evidence-confidence indicators;
- recommended mitigation options and estimated costs;
- a record of human review and accepted or rejected recommendations.

Implementation requires reliable entity identifiers, timestamped observations, versioned dependency records, access-controlled data storage, and documented model assumptions. A model that cannot explain why a risk estimate changed will be difficult to trust, even if its underlying calculations are mathematically sound.

4.7 Reproducibility and Operational Governance

The model should maintain a versioned record of its data, assumptions, inference rules, and evaluation results. Each risk estimate should be reproducible using the evidence available at the time of assessment. Governance should establish responsibility for validating incoming information, approving material changes to the model,

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

investigating false positives, and reviewing high-impact recommendations. The organization should also periodically test whether the model remains useful as the supply chain and threat environment evolve.

V. DISCUSSION

5.1 Interpreting the Proposed Contribution

The central contribution of CTCRAM is its proposed integration of changing security evidence, dependency relationships, probabilistic risk estimation, and mitigation decisions. These elements address different weaknesses in third-party cyber risk management and should be evaluated both individually and collectively.

The model's value would not lie merely in producing more frequent risk scores. It would lie in connecting a change in observed conditions to a defensible explanation of how organizational exposure may have changed. For example, a newly disclosed vulnerability becomes materially important when the affected component is deployed, the relevant attack pathway is plausible, and the connected business service has meaningful consequences. This contextual approach is consistent with the wider direction of supply chain cybersecurity guidance, which emphasizes understanding external dependencies and integrating supplier risk into organizational decision-making (Boyens et al., 2022; NIST, 2024a).

5.2 The Importance of Network-Aware Assessment

A network perspective offers a way to identify exposures that are difficult to capture through independent vendor assessments. Shared cloud providers, identity services, software libraries, and managed service providers may create common points of failure.

Nevertheless, a network-aware model is not automatically more accurate. Its performance depends on the quality of the relationship data, the plausibility of the propagation assumptions, and the treatment of common-cause events. An incomplete graph can create a misleading picture of isolation, while indiscriminate propagation can exaggerate risk.

The implication is that network modelling should be combined with contextual evidence and tested against simpler approaches. The objective is not to maximize the number of relationships represented but to identify those relationships that materially affect exposure and consequences.

5.3 Continuous Assessment and Organizational Decision-Making

Continuous assessment could help organizations move from a predominantly review-based process toward more responsive risk management. Yet automation introduces its own challenges. Frequent alerts can overwhelm analysts, and a rapidly changing numerical score may undermine confidence if its drivers are not transparent.

For this reason, risk changes should be accompanied by explanations. The system should identify the new evidence, the affected dependency, the relevant scenario, and the estimated effect on organizational loss. It should also distinguish high-risk situations from cases in which uncertainty is simply high.

Human oversight remains essential where supplier termination, service interruption, regulatory reporting, or major financial commitments are involved. The model should support informed decisions, not obscure accountability behind an automated recommendation.

5.4 Implications for Cybersecurity Investment

The proposed model could improve the allocation of cybersecurity resources by connecting mitigation actions to estimated changes in expected loss. For instance, removing unnecessary privileged access may be more economical than replacing a supplier, while a critical shared dependency may justify investment in redundancy or a tested recovery arrangement.

However, expected-loss minimization is not the only legitimate objective. Organizations must also consider legal obligations, operational resilience, customer trust, safety, and risk appetite. A low-cost mitigation may be unacceptable if it leaves a mandatory control unmet or exposes the organization to an intolerable disruption.

Consequently, the model should combine quantitative estimates with explicit constraints and documented management judgment. Its purpose is to make trade-offs clearer, not to reduce every decision to a single financial score.

5.5 Governance, Data Sharing, and Trust

Continuous third-party risk assessment depends on information that may be sensitive to suppliers. Organizations may need details about vulnerabilities, software components, access privileges, and security incidents that vendors are reluctant or unable to share fully.

A practical implementation must therefore define what information is necessary, who can access it, how long it is retained, and how disagreements about its accuracy are resolved. Suppliers should have a reasonable mechanism to correct material errors, particularly when an assessment could affect a significant commercial relationship.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Data sharing also needs to be proportionate. More data do not always produce better decisions if they are unreliable, duplicative, or irrelevant. The governance challenge is to obtain sufficiently informative evidence while protecting confidentiality and maintaining manageable operational requirements.

5.6 Limitations and Interpretation of Evidence

The proposed framework faces several limitations.

First, incident data may be sparse and inconsistently reported. This restricts the ability to estimate precise probabilities and validate predicted losses. Second, vendor and software dependency records may be incomplete, particularly where subcontractors and indirect services are involved. Third, propagation assumptions may simplify real attack paths, which can depend on attacker behaviour, defensive controls, and organizational responses.

Fourth, simulated evaluation may not capture the full complexity of operational environments. A model can perform well in a controlled simulation because its assumptions are known and its data are internally consistent. Real environments contain missing observations, conflicting records, adaptive adversaries, and organizational constraints that are difficult to reproduce.

Finally, the integration of several modelling methods increases maintenance demands. An organization must be able to update data pipelines, monitor calibration, validate changes, and explain model outputs. The benefits of continuous assessment should therefore be weighed against the cost and complexity of maintaining it.

VI. RECOMMENDATIONS AND IMPLICATIONS

6.1 Recommendations for Organizations

Organizations considering continuous third-party cyber risk assessment should begin with the dependencies that matter most to their operations rather than attempting to model every supplier in equal detail.

First, establish a reliable inventory of critical vendors, software components, third-party accounts, and business services. Prioritize relationships involving sensitive information, privileged access, essential operations, or limited alternatives.

Second, connect existing information sources where feasible. Procurement systems, vulnerability management tools, software inventories, and access-management records should use consistent identifiers and timestamps so that relevant changes can be traced to affected services.

Third, define material-change triggers. Examples include a confirmed supplier compromise, a critical vulnerability in a deployed dependency, an unexpected expansion of privileged access, or evidence that a critical provider is experiencing a major service disruption. Trigger definitions should reflect organizational risk appetite and the quality of available evidence.

Fourth, retain human review for uncertain or high-impact cases. Automated systems should flag relevant evidence, explain estimated changes, and identify missing information. Analysts should validate material findings before consequential decisions are made.

Fifth, evaluate whether continuous assessment improves actual decision quality. Organizations should monitor reassessment latency, false alerts, missed exposures, model calibration where measurable, and the costs of maintaining the system.

6.2 Recommendations for Vendor and Software Monitoring

Vendor monitoring should extend beyond annual questionnaires. Periodic assurance remains important, but it should be supplemented by credible information about security incidents, access changes, relevant control weaknesses, and changes in service criticality.

For software dependencies, organizations should maintain current component inventories where technically and contractually feasible. SBOMs should be linked to vulnerability information and asset inventories, with validation to establish whether affected components are deployed and relevant.

Third-party access should be reviewed according to privilege, sensitivity, and business need. Unnecessary permissions should be removed, and material changes should be recorded so that the risk model can distinguish current exposure from historical access.

Organizations should also assess concentration risk. If several critical services depend on the same provider, the appropriate response may involve stronger controls, contingency planning, tested recovery arrangements, or alternative service options rather than simply assigning the provider a higher numerical score.

6.3 Recommendations for Model Governance

A continuous assessment programme should have clearly assigned responsibility for data quality, model validation, risk escalation, and mitigation decisions.

The organization should document the meaning of its risk measures, the assumptions underlying scenario probabilities, the treatment of uncertainty, and the circumstances in which a human override is permitted. Material model changes should be tested before deployment and recorded for auditability.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Model performance should be reviewed periodically. If prediction quality deteriorates, dependency records become stale, or recommendations repeatedly prove unhelpful, the organization should investigate and recalibrate the model rather than assume that automation guarantees accuracy.

6.4 Recommendations for Future Research

Future research should evaluate the proposed model using longitudinal organizational data and documented incident outcomes. Such studies would help determine whether continuous assessment improves real-world risk recognition and mitigation rather than only performance in simulated environments.

Cross-industry comparisons could examine whether the model performs differently in finance, healthcare, manufacturing, education, and cloud-dependent professional services. These environments vary in regulatory obligations, operational criticality, supplier concentration, and tolerance for disruption.

Further work should also investigate privacy-preserving approaches to sharing supplier risk information, methods for representing fourth-party dependencies, and techniques for estimating correlated losses. Another important direction is to examine the cost-effectiveness of continuous assessment relative to simpler monitoring and periodic review arrangements.

Finally, researchers should study how organizations interpret model outputs and incorporate them into governance. Technical accuracy is important, but a model that produces poorly explained recommendations or excessive alerts may fail to improve decisions in practice.

VII. CONCLUSION

For organizations using interconnected vendors, software components, cloud services and reliant on outside access relationships, third-party cyber risk is a growing problem. These dependencies can pose exposure that shifts with the discovery of new vulnerabilities, the growth of privileges, incidents in suppliers, and the development of new business relationships. While periodic assessments can provide good security baselines, they cannot capture material changes between periodic reviews, and do not adequately reflect indirect exposures via shared dependencies.

In this study, a continuous third-party cyber risk assessment model is proposed, which integrates event-triggered updates, a time-dependent dependency graph, probabilistic incident estimation, uncertainty representation, and decision support on mitigation. The idea is that the risk of an organization in cyberspace should be assessed based on the changing nature of the external entities, the nature of their relationships, the quality of available evidence, and the implications of likely scenarios of incidents.

It is also proposed that continuous monitoring is not enough in itself and the monitoring model should be continuous. Relevant data, defensible estimates of the likelihood of events, explicit handling of correlated events, transparent assumptions, and appropriate oversight by humans are needed for better assessment. Network analysis can be used to determine indirect exposure but the results are only as accurate as the information about dependencies in the network. Probabilistic modelling can be used to model uncertainty, but not uncertainty that the evidence available does not resolve.

The planned contribution is not about proving a superior approach, but an integrated and testable approach. The model should be compared with network-aware and network-independent versions which are static, periodic, and dynamic and, when appropriate, be compared to models that are not network-aware, keeping all the following in mind: Consistent data, appropriate performance metrics, and clear assumptions. If conclusions are drawn based on synthetic scenarios, the conclusions should be restricted to those scenarios until they are tested in operational scenarios.

In conclusion, third-party cyber risk assessment is a promising tool to link evolving security evidence to organizational decisions. How useful it will be to them will rely on whether they can identify material changes earlier, estimate exposure more defensibly, prioritize mitigation more effectively and keep a clear understanding of the dependencies on which their digital operations are reliant.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

REFERENCES

1) Anderson, R. (2001). Why information security is hard—An economic perspective. In Proceedings of the 17th Annual Computer Security Applications Conference (pp. 358–365). IEEE. https://doi.org/10.1109/ACSAC.2001.991552
2) Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). Cybersecurity supply chain risk management practices for systems and organizations (NIST Special Publication 800-161 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1
3) Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342–353. https://doi.org/10.1016/j.technovation.2014.02.001
4) Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. Future Internet, 15(10), Article 324. https://doi.org/10.3390/fi15100324
5) Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. Journal of Financial Economics, 147(2), 432–448. https://doi.org/10.1016/j.jfineco.2022.12.002
6) Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105. https://doi.org/10.2307/25148625
7) Hubbard, D. W., & Seiersen, R. (2016). How to measure anything in cybersecurity risk. Wiley.
8) International Organization for Standardization. (2018). ISO 31000:2018 risk management—Guidelines.
9) International Organization for Standardization. (2022). ISO/IEC 27005:2022 information security, cybersecurity and privacy protection—Guidance on managing information security risks.
10) Koller, D., & Friedman, N. (2009). Probabilistic graphical models: Principles and techniques. MIT Press.
11) National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1
12) National Institute of Standards and Technology. (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (NIST Special Publication 800-37 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2
13) National Institute of Standards and Technology. (2022). Software security in supply chains: Software bill of materials (SBOM). U.S. Department of Commerce. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-supply-chain-security-guidance-20
14) National Institute of Standards and Technology. (2024a). Cybersecurity Framework 2.0: Quick-start guide for cybersecurity supply chain risk management (C-SCRM) (NIST Special Publication 1305). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.1305
15) National Institute of Standards and Technology. (2024b). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
16) Newman, M. (2018). Networks (2nd ed.). Oxford University Press.
17) Pearl, J. (1988). Probabilistic reasoning in intelligent systems: Networks of plausible inference. Morgan Kaufmann.
18) Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302
19) Reichert, B. M., & Obelheiro, R. R. (2024). Software supply chain security: A systematic literature review. International Journal of Computers and Applications, 46(10), 853–867. https://doi.org/10.1080/1206212X.2024.2390978
20) Vose, D. (2008). Risk analysis: A quantitative guide (3rd ed.). Wiley.
21) Xia, B., Bi, T., Xing, Z., Lu, Q., & Zhu, L. (2023). An empirical study on software bill of materials: Where we stand and the road ahead. In Proceedings of the 45th IEEE/ACM International Conference on Software Engineering. IEEE/ACM. https://doi.org/10.1109/ICSE48619.2023.00219

 © Author(s) | CC BY 4.0 International License.