**Systemy Logistyczne Wojsk**
Zeszyt 64(2026)
ISSN 1508-5430, s. 141-156
DOI: 10.37055/slw/224978

Instytut Logistyki
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

**Military Logistics Systems**
Volume 64(2026)
ISSN 1508-5430, pp. 141-156
DOI: 10.37055/slw/224978

Institute of Logistics
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

# CYBERSECURITY RISK ASSESSMENT OF SUPPLIERS IN THE SUPPLY CHAIN USING THE AHP METHOD AND A SCORING MODEL

**Mateusz Zawadzki**

mateusz.zawadzki02@wat.edu.pl; ORCID: 0009-0002-0737-1210
Faculty of Security, Logistics and Management, Military University of Technology, Poland

**Abstract.**
The article addresses the problem of cybersecurity risk in digitally interconnected supply chains, with particular emphasis on supplier relationships, third-party access and software dependencies. The research niche of this study is the operationalisation of publicly available cyber-risk data into a transparent and reproducible assessment model that can be applied without access to confidential company datasets. The purpose of the article is to develop a multi-criteria model for assessing supplier cybersecurity risk using the Analytic Hierarchy Process (AHP) and a scoring procedure grounded in recognised reports and scientific literature, and to demonstrate its application in an illustrative supply-chain context. The main hypothesis assumes that supplier cyber risk can be systematically compared through the integration of threat exposure, technical vulnerability and operational impact within a structured weighted index. The study applies a mixed-method approach, including literature review, comparative analysis, desk research, mathematical modelling, AHP weighting and sensitivity analysis. Empirical input was derived from NIST guidance, the ENISA report on supply chain attacks, Verizon's 2025 Data Breach Investigations Report and IBM's 2025 Cost of a Data Breach Report. The results indicate that transportation and utilities suppliers achieve the highest risk levels in the illustrative application, while ICT suppliers remain highly critical in terms of digital dependency. The conclusions support the usefulness of the proposed model as a preliminary decision-support framework, while indicating the need for further expert-panel and organisation-specific validation.
**Keywords:**
cybersecurity; supply chain; supplier risk; AHP; cyber risk assessment

## Introduction

The digitalisation of supply chains has profoundly changed the nature of operational risk. Contemporary organisations rely not only on their own information systems but also on cloud service providers, software vendors, managed service partners, logistics operators, industrial utilities and subcontractors that process data or support mission-critical processes. As a result, the cyber resilience of a focal organisation increasingly depends on the security posture of entities outside its formal boundaries (Christopher 2016; Sheffi 2005). The National Institute of Standards and Technology (NIST) defines cybersecurity supply chain risk management as a multi-level approach to identifying, assessing and mitigating cybersecurity risks throughout the supply chain and explicitly integrates it with enterprise risk management (Boyens et al. 2022). This shift is especially important in sectors where digital disruption can immediately affect production, logistics, public services or critical infrastructure (Ivanov 2021).

Recent studies published in Military Logistics Systems also confirm that the growing digitalisation of logistics systems increases both operational efficiency and exposure to cybersecurity threats. Innovative logistics technologies such as AI-supported monitoring systems, intelligent warehousing and integrated digital platforms improve supply-chain performance but simultaneously increase dependence on interconnected IT and OT environments, thereby expanding the cyber-risk surface of logistics operations (Ismayilov et al. 2025).

The relevance of the problem has been reinforced by attacks that exploit trusted supplier relationships and third-party dependencies. The ENISA report on supply chain attacks provides a dedicated empirical basis for understanding how supplier trust, supplier code and advanced persistent threat activity can be used as attack vectors in interconnected systems (ENISA 2021). Although this source refers to the 2020-2021 period, it remains relevant for the present study because it provides specific quantitative indicators directly related to supply chain attacks. More recent cross-sectoral evidence from Verizon confirms that third-party involvement in breaches remains an important dimension of contemporary cybersecurity risk (Verizon 2025).

The academic challenge lies in transforming dispersed observations into an operational assessment instrument. Fewer studies show how to derive a transparent comparative model from accessible secondary data (Heckmann et al. 2015; Boyson 2014). This article addresses that gap by proposing an illustrative framework for preliminary supplier cyber-risk comparison (Tang 2006).

## Purpose of the article, research problem and hypothesis

The purpose of the article is to develop a transparent method for assessing the cybersecurity risk of suppliers in a digitally interconnected supply chain and to demonstrate how public secondary data can be transformed into a weighted comparative ranking. The central research problem may be formulated as follows: how can the cybersecurity risk of different categories of suppliers be assessed and compared on the basis of recognised reports, normative guidance and multi-criteria decision methods?

Three research questions follow from this problem. First, which criteria are the most significant in supplier cyber-risk assessment? Second, can a coherent scoring model be constructed from publicly available data without access to confidential company records? Third, which supplier category reaches the highest risk level when the model is applied in an illustrative demonstration?

The main hypothesis states that supplier cybersecurity risk can be systematically and analytically compared by combining three dimensions: threat exposure, technical vulnerability and operational impact. An auxiliary hypothesis assumes that the AHP method provides a structured basis for weighting these criteria, while publicly documented cyber reports contain sufficient information to calibrate an illustrative model application. The hypothesis is therefore examined within the scope of a methodological demonstration rather than through full empirical validation based on organisation-specific audit data.

## Research methods

The article adopts a mixed research strategy with a dominant quantitative component. The first method is a structured literature review aimed at identifying conceptual approaches to supply chain risk management and cyber supply chain risk management (Heckmann et al. 2015; Colicchia and Strozzi 2012). The second is desk research based on documents issued by NIST, ENISA, Verizon and IBM (ENISA 2021; Verizon 2025; IBM 2025). The third method is comparative analysis, which is used to transform source indicators into comparable scales. The fourth is mathematical modelling, in which a scoring index is constructed from normalised variables (Tang 2006). The fifth method is the Analytic Hierarchy Process, used to determine the relative weights of the risk criteria (Saaty 1987; Saaty 2008).

In the present study, the AHP pairwise-comparison matrix was constructed by the author on the basis of the reviewed literature, institutional cybersecurity risk frameworks and empirical indicators used in the model. Therefore, the weighting procedure should be understood as a structured expert-informed judgement rather than as a multi-expert panel assessment. This limitation is explicitly acknowledged

and provides a basis for further development of the model through expert-panel aggregation in future research.

The article does not aim to provide a full organisational audit or a validated predictive tool; rather, it presents a structured modelling approach that can be further developed using internal data, expert surveys, sector-specific indicators or audit-based evidence. Such an approach is aligned with the principles of ISO/IEC 27005, which treats risk identification, analysis, evaluation and treatment as an iterative process supported by quantitative and qualitative information (ISO/IEC 2022; Boyens et al. 2022).

## Literature review

The theoretical point of departure is the broader literature on supply chain risk management. Supply chains become more efficient and more vulnerable as they rely on outsourcing, globalisation and network complexity (Tang 2006). Resilience-oriented and network-based perspectives are therefore central to the discipline (Colicchia and Strozzi 2012; Ivanov 2021). Network complexity, upstream dependency and system viability have also been identified as important dimensions of disruption risk (Bode and Wagner 2015; Pettit et al. 2010; Ivanov and Dolgui 2020).

Cyber supply chain risk management extends classical supply chain risk concepts into the domain of information security, software assurance and third-party digital dependencies. Boyson described cyber supply chain risk management as an integrative discipline linking cybersecurity, supply chain management and enterprise risk management (Boyson 2014). This approach is reinforced by NIST, which recommends integrating C-SCRM into organisational governance, acquisition, supplier management, systems development and enterprise-wide risk decision-making (Boyens et al. 2022).

A growing body of literature and policy evidence shows that cyber incidents increasingly propagate through trusted relationships. Research and reports emphasise software dependencies, open-source components, supplier credentials, managed service providers and weakly governed third-party access as common attack channels (ENISA 2021; Verizon 2025). ENISA's later guidance on good practices for supply chain cybersecurity further underlines governance, supplier relationship management, verification and secure engineering as core domains of defence (ENISA 2023). Recent publications in *Military Logistics Systems* also emphasise that digital technologies in logistics systems increase both efficiency and exposure to cyber-related risks (Ismayilov et al. 2025). Recent research in *Military Logistics Systems* also links logistics resilience with crisis conditions and continuity-oriented management, which is relevant for interpreting cyber disruption as a risk to logistics-system continuity (Jałowiec and Spychalski 2025).

From a methodological point of view, the AHP method is suitable because supplier cyber risk is a multi-criteria problem in which not all determinants can be measured in the same unit. AHP allows pairwise comparisons among criteria and provides a consistency ratio that helps assess whether the weighting logic is coherent. The method has been widely used in risk analysis and decision support because it combines mathematical tractability with managerial interpretability (Saaty 1987; Saaty 2008).

## State of knowledge

The current state of knowledge indicates three consistent findings. First, cyber risk in supply chains is rising and cannot be analysed solely within the boundaries of a single organisation (Ivanov 2021; Tang 2006). Second, the most significant attack channels increasingly involve supplier trust, third-party access or exploitable software dependencies (Boyson 2014; ENISA 2021). Third, organisations still face a methodological gap between strategic recommendations and operational ranking tools (Heckmann et al. 2015).

NIST stresses that supply-chain products and services may contain malicious functionality or vulnerabilities caused by poor development and manufacturing practices (Boyens et al. 2022). ENISA shows that advanced actors exploit trust relationships and supplier software channels (ENISA 2021), while Verizon and IBM provide recent evidence on breaches, vulnerability exploitation and financial consequences (Verizon 2025; IBM 2025).

Despite these advances, the literature still often separates governance recommendations from scoring models. Scientific articles frequently discuss what should be monitored, while practitioner reports describe what was observed, but fewer studies demonstrate how dispersed secondary data can be transformed into a transparent comparative assessment procedure (Colicchia and Strozzi 2012; Heckmann et al. 2015). The present article contributes to this gap by proposing a structured operationalisation pathway: source data are identified, converted into indicators, weighted with AHP and aggregated into a supplier cyber-risk index. This contribution should be understood as a methodological framework for preliminary comparison rather than as a substitute for organisation-specific supplier audit.

## Data sources and the logic of indicator construction

The empirical input consists exclusively of secondary data. This choice increases transparency, enables replication and avoids the confidentiality problems that often limit cyber-risk research at company level. At the same time, it requires explicit

separation between source data and model assumptions. In this article, all primary numerical observations are taken from recognised external publications, whereas aggregation weights and certain normalisation decisions are the author's analytical contribution.

Four groups of sources were used. NIST and ISO/IEC justify the model structure and the inclusion of supplier criticality (Boyens et al. 2022; ISO/IEC 2022). ENISA provides supply-chain attack indicators, including supplier-trust exploitation, supplier-code compromise and APT attribution (ENISA 2021). Verizon provides breach and vulnerability evidence, while IBM anchors the impact dimension through breach-cost data (Verizon 2025; IBM 2025).

A temporal asymmetry exists between ENISA 2021 and the more recent Verizon and IBM 2025 reports. ENISA 2021 was retained because it provides specific numerical indicators for supply-chain attacks. More recent ENISA evidence, including the Threat Landscape 2025 analysis of 4875 incidents, confirms the continuing relevance of cyber threats in interconnected environments (ENISA 2025).

The article does not claim that the reports contain complete records for named suppliers. Instead, sectoral and cross-sectoral evidence is transformed into an illustrative application for three supplier categories: ICT, transportation and utilities suppliers. The model is a methodological demonstration and preliminary decision-support framework rather than a validated predictive tool.

## Transparency of variables, sources and assumptions

Table 1. Sources, transformations and assumptions used in the model

| Variable / parameter | Role in model | Source | Transformation / normalisation | Author-defined assumption |
|---|---|---|---|---|
| Supplier-trust exploitation; supplier-code focus; APT attribution | Components of | ENISA (2021) | Used directly as normalised shares | No |
| Fourfold increase indicator | Component of | ENISA (2021) | Normalised to 1.00 as maximum trend intensity | Yes - scaling decision |
| Transport sector indicators | Components of | Verizon (2025) | Pattern concentration and external actor shares used directly; breach-to-incident ratio converted to 0.687 | No |
| Utilities sector indicators | Components of | Verizon (2025) | Pattern concentration and external actor shares used directly; breach-to-incident ratio converted to 0.595 | No |

| | | | | |
|---|---|---|---|---|
| Vulnerability exploitation and edge-device/VPN exploitation | Components of | Verizon (2025) | Used directly as normalised shares | No |
| Remediation completion and median remediation time | Components of | Verizon (2025) | Unresolved share calculated as 1 - 0.54; remediation time normalised as 32/90 = 0.356 | Benchmark selection |
| Digital-dependence multipliers: ICT 1.8, transport 1.2, utilities 1.3 | Adjustment of | Author-defined | Applied to | Yes |
| Impact scores: ICT 0.95, transport 0.80, utilities 0.90 | Components of | IBM (2025), Boyens et al. (2022), author judgement | Categorical criticality scores | Yes |
| AHP weights: = 0.637, = 0.258, = 0.105 | Criterion weights | Saaty (1987, 2008), author judgement | Eigenvector method | Yes |

Source: own elaboration

Table 1 separates source-derived parameters from author-defined modelling assumptions. This distinction is essential because the proposed framework combines empirical indicators with structured analytical judgement. Source-derived parameters were taken directly from institutional reports or converted into ratios, whereas author-defined assumptions were introduced only where comparable sector-specific data were unavailable.

## Model construction

The model is based on three criteria: threat exposure, technical vulnerability and operational impact. Threat exposure reflects observed attack patterns, vulnerability reflects exploitable weaknesses and patching gaps, while impact reflects potential disruption to continuity, data integrity or service availability. The proposed cyber risk assessment model is expressed as:

$$CR_i = w_T \cdot T_i + w_V \cdot V_i + w_I \cdot I_i \tag{1}$$

where $CR_i$ represents the overall cyber risk level associated with supplier category $i$, while ,

and denote the normalised values of threat, vulnerability, and impact respectively, within the range [0,1]. The weights $w_T, w_V, w_I$ reflect the relative importance of each criterion and are determined using the Analytic Hierarchy Process.

The model is based on a synthetic aggregation of three key dimensions: threat, vulnerability

and impact. Each component was constructed as a composite indicator derived from empirical data and established risk assessment frameworks. The additive structure was selected because it is transparent and interpretable. Multiplicative formulations could amplify extreme values and would be less suitable for a preliminary demonstration based on heterogeneous secondary data. The model should therefore be interpreted as a structured analytical framework intended for preliminary comparison rather than as a fully validated predictive tool.

The relative importance of each component was determined using AHP. Threat exposure was assessed as moderately more important than technical vulnerability and strongly more important than operational impact, because current breach evidence shows that attack channels and exploitability trends are the main drivers of incident initiation. Technical vulnerability was assessed as more important than impact because a high-impact supplier that is very difficult to compromise does not necessarily represent the highest immediate cyber risk. This yields matrix A:

$$A = \begin{bmatrix} 1 & 3 & 5 \\ 1/3 & 1 & 3 \\ 1/5 & 1/3 & 1 \end{bmatrix}$$

The pairwise-comparison matrix was constructed by the author on the basis of literature, institutional frameworks and empirical indicators. Therefore, the AHP procedure should be interpreted as structured expert-informed judgement rather than as a multi-expert panel assessment. Future research should use expert-panel aggregation, for example the geometric mean of individual judgements.

After normalisation of matrix A, the resulting weight vector is = 0.637, = 0.258 and = 0.105. The calculated consistency ratio is approximately 0.033, which remains below the usual acceptability threshold of 0.10. This indicates that the weighting structure is internally consistent within the adopted pairwise-comparison matrix. However, because the matrix was based on structured author judgement, the resulting weights should be treated as a transparent methodological proposal rather than as universal criterion weights.

The threat-exposure indicator for the ICT supplier category was derived from ENISA. Four source values were used: 0.62 for attacks exploiting trust in the supplier, 0.66 for incidents focused on supplier code, 0.50 for attacks attributed to APT actors and a trend-dynamics factor based on the reported fourfold increase in supply-chain attacks. The trend factor was normalised to 1.00 so that all components could be expressed on the same 0-1 scale.

$$T_{ICT} = 0.30 \cdot 0.62 + 0.30 \cdot 0.66 + 0.20 \cdot 0.50 + 0.20 \cdot 1.00 = 0.684$$

The transportation and utilities supplier categories were calibrated primarily with Verizon sectoral evidence. For transportation, the indicator combines 0.91 for the share of breaches concentrated in three dominant attack patterns, 0.94 for the share attributable to external actors and the ratio of confirmed breaches to recorded incidents. For utilities, the same logic was applied with 0.92 for dominant-pattern concentration, 0.92 for external actors and the breach-to-incident ratio 213/358.

$$T_{TRANS} = 0.40 \cdot 0.91 + 0.30 \cdot 0.94 + 0.30 \cdot (248/361) = 0.852$$

$$T_{UTIL} = 0.40 \cdot 0.92 + 0.30 \cdot 0.92 + 0.30 \cdot (213/358) = 0.823$$

The technical-vulnerability baseline was calculated from Verizon's broader breach indicators: vulnerability exploitation as an initial access vector, edge-device and VPN-related exploitation, the unresolved portion of vulnerabilities and normalised remediation time. A 90-day denominator was adopted as a conservative benchmark for a delayed but still operationally interpretable response window.

$$V_{BASE} = 0.35 \cdot 0.20 + 0.25 \cdot 0.22 + 0.20 \cdot (1 - 0.54) + 0.20 \cdot (32/90) = 0.288$$

$$V_i = V_{BASE} \cdot m_i \quad (2)$$

The adopted multipliers are 1.8 for ICT suppliers, 1.2 for transportation suppliers and 1.3 for utilities suppliers. These multipliers are not directly reported in external sources; they are an analytical component of the model and reflect the degree to which each supplier category depends on continuously exposed digital infrastructure, software administration and remote connectivity.

Operational impact was anchored conceptually in NIST's emphasis on critical suppliers and materially in IBM's finding that the global average cost of a breach reached USD 4.4 million in 2025. Because IBM does not provide a directly comparable cost value for each supplier category in the present model, the impact score was assigned through explicit categorical criticality assessment rather than false precision. The values adopted were 0.95 for ICT suppliers, 0.80 for transportation suppliers and 0.90 for utilities suppliers.

## Illustrative application of the model in an industrial supply chain context

To demonstrate the practical use of the proposed framework, an illustrative application was developed based on a representative industrial supply-chain structure. This section should not be interpreted as a full empirical case study of a specific organisation or as validation based on original organisational data. Its purpose is to show how the proposed model can be applied to supplier categories under transparent and reproducible assumptions.

ICT suppliers are responsible for critical digital services, including cloud infrastructure, software delivery and identity management systems. Transportation suppliers ensure the continuity of logistics and distribution processes, while utilities providers support the uninterrupted supply of energy and technical infrastructure. These supplier categories were selected because they represent distinct yet interdependent layers of exposure within modern cyber-physical systems.

The calculated threat levels were = 0.684, = 0.852 and = 0.823. The corresponding vulnerability values were = 0.518, = 0.346 and = 0.374. The impact scores were = 0.950, = 0.800 and = 0.900. Based on these inputs, the final cyber risk scores were = 0.669, = 0.716 and = 0.715.

The ranking should be interpreted carefully. ICT suppliers receive the highest operational impact score in the model because they are strongly connected with software infrastructure, identity management and digital dependency. Their lower aggregate ranking results from the interaction between all three model dimensions and does not imply lower criticality. Rather, it shows that the final score depends on the combined effect of threat exposure, technical vulnerability and operational impact.

## Results

The application of formula (1) with the calculated weights and normalised indicator values yields the illustrative ranking shown in Table 2. To ensure transparency and reproducibility of the calculation procedure, the weighted sums are presented explicitly:

$$CR_{ICT} = 0.637 \cdot 0.684 + 0.258 \cdot 0.518 + 0.105 \cdot 0.950 = 0.669$$

$$CR_{TRANS} = 0.637 \cdot 0.852 + 0.258 \cdot 0.346 + 0.105 \cdot 0.800 = 0.716$$

$$CR_{UTIL} = 0.637 \cdot 0.823 + 0.258 \cdot 0.374 + 0.105 \cdot 0.900 = 0.715$$

The final ranking should not be interpreted as an arbitrary assignment. It results from a sequential procedure involving the selection of source statistics, normalisation where required, weighted aggregation into threat and vulnerability indicators, categorical criticality-based assignment of impact scores, derivation of criterion weights by AHP and calculation of the weighted sum in formula (1).

The illustrative ranking shows that transportation suppliers obtain the highest score of 0.716, closely followed by utilities suppliers at 0.715. ICT suppliers reach 0.669, which also indicates a high level of cyber risk under the adopted scoring assumptions. The narrow difference between transportation and utilities suggests that both categories should be treated as high-priority supplier groups in operational environments dependent on physical continuity, service availability and rapid incident containment.

The ranking should be interpreted carefully. ICT suppliers receive the highest operational impact score in the model because they are strongly connected with software infrastructure, identity management and digital dependency. Their lower aggregate score results from the interaction between all three model dimensions and does not imply lower criticality. In organisations where software concentration risk or identity infrastructure dependency dominates the business model, the ranking could change after recalibration with organisation-specific data.

Table 2. Supplier-category cyber-risk assessment results

| Supplier category | T | V | I | CR |
|---|---|---|---|---|
| ICT supplier | 0.684 | 0.518 | 0.950 | 0.669 |
| Transportation supplier | 0.852 | 0.346 | 0.800 | 0.716 |
| Utilities supplier | 0.823 | 0.374 | 0.900 | 0.715 |

Source: own elaboration based on Boyens et al. (2022), ENISA (2021), Verizon (2025) and IBM (2025)

## Sensitivity analysis and robustness assessment

To assess the internal robustness of the proposed scoring procedure, a sensitivity analysis was conducted by varying the AHP-derived criterion weights within a +/-10% range while preserving their relative ordering. This procedure should not be interpreted as full empirical validation of the model, because no organisation-specific audit data, incident records or independent expert-panel dataset were used at this stage. Rather, it provides an internal robustness check showing whether moderate changes in the adopted weights substantially affect the illustrative ranking of supplier categories. After a 10% increase in the impact weight and re-normalisation

of the weight vector, utilities slightly exceeded transportation, whereas after a 10% increase in the threat weight, transportation remained first. In all tested variants, ICT suppliers remained third, which indicates that the model preserves the distinction between digitally critical and operational-continuity-oriented supplier categories.

The results indicate that the ranking remains broadly stable under moderate changes in weight values. Increasing the weight of threat exposure strengthens the relative position of transportation suppliers, while increasing the weight of operational impact slightly increases the relative position of utilities suppliers. No tested configuration resulted in a complete reversal of the ranking.

These findings suggest that the scoring procedure is internally consistent within the adopted assumptions. However, the results should be interpreted as a robustness assessment of an illustrative model application rather than as empirical validation of a predictive tool. Further validation would require organisation-specific supplier data, audit-based evidence or expert-panel assessment.

## Discussion

The findings support the main hypothesis within the scope of the adopted methodological framework. The results indicate that supplier cyber risk can be compared in a structured way when three conditions are met: the criteria are conceptually grounded, the weighting procedure is explicitly justified, and the transformation from source data to analytical indicators is transparent. The proposed model addresses these conditions by combining literature-based criteria, AHP-derived weights and clearly described data transformation procedures. However, the obtained results should be interpreted as an illustrative comparative assessment rather than as empirical validation of a predictive model.

The analysis also highlights an important methodological issue concerning the use of secondary data in cyber supply chain risk assessment. The values applied in the model are derived from recognised institutional sources and are combined with explicitly identified author-defined assumptions. The analytical contribution of the study lies in the structured transformation of these inputs into normalised and aggregated indicators, while clearly distinguishing source-derived parameters from assumptions introduced by the author.

From a methodological perspective, the proposed framework demonstrates how dispersed secondary data can be operationalised into a preliminary supplier-risk comparison. This is particularly relevant where organisation-specific audit data, real-time telemetry or proprietary incident records are unavailable. At the same time, the model should not be treated as a substitute for supplier audits, penetration testing, contractual due diligence, expert-panel assessment or real-time threat

intelligence. Its primary value lies in structuring the assessment process, supporting preliminary prioritisation and making assumptions explicit.

Cyber threat exposure, vulnerability patterns and operational impact may change as new attack techniques, digital dependencies and supplier relationships emerge. Consequently, the results should be interpreted as context-dependent and subject to periodic recalibration. As new empirical data become available or organisation-specific information is incorporated, the model can be updated without altering its conceptual structure.

## Practical implications for supplier governance

The proposed framework may support supplier governance as a preliminary decision-support tool. The identification of higher-risk supplier categories may justify enhanced due diligence, more detailed contractual requirements and closer monitoring of suppliers that influence operational continuity. However, these actions should be treated as risk-informed indications rather than automatic prescriptions generated by the model.

For suppliers with high operational criticality, the results suggest the need for an integrated assessment of cybersecurity and business continuity capabilities. In sectors such as transportation or utilities, supplier evaluation may therefore extend beyond information security to include the ability to maintain or restore services under disruption conditions. At the same time, ICT suppliers should not be interpreted as less critical simply because their aggregate score is lower in the illustrative application.

The framework may also constitute a conceptual basis for future AI-supported and Big Data-driven supplier risk assessment systems. Such systems could integrate real-time threat intelligence, supplier telemetry, vulnerability scanning results, incident-history data and automated anomaly detection mechanisms. In this sense, the model should be understood as a transparent methodological foundation that can be expanded into more data-intensive and operationally mature tools.

## Limitations of the study

The study has several limitations. First, it relies on secondary data from institutional reports rather than proprietary datasets, supplier audits or organisation-specific incident records. This increases transparency and reproducibility, but the results should be treated as an illustrative comparison rather than a direct diagnosis of any specific organisation or supplier.

Second, selected elements of the model are based on structured analytical judgement, especially the digital-dependence multipliers, impact scores and remediation-time benchmark. These assumptions were introduced because comparable sector-specific datasets were unavailable and should be refined through expert panels, audit evidence or sector-specific data.

Third, the AHP matrix was constructed by the author as structured expert-informed judgement rather than through a multi-expert panel. Although the consistency ratio indicates internal coherence, the resulting weights should not be interpreted as universal criterion weights. Future studies should use group AHP procedures involving cybersecurity, logistics, procurement and risk-management experts.

Fourth, the study combines data sources that differ in temporal scope and analytical perspective. The ENISA 2021 report was retained because it provides specific numerical indicators for supply chain attacks, while Verizon and IBM 2025 offer more recent cross-sectoral evidence on breaches, vulnerabilities and financial consequences. This temporal asymmetry should be considered when interpreting the results. Finally, the application of the model should be understood as an illustrative demonstration rather than a full empirical case study.

Future research may further develop the model by incorporating primary data sources, such as expert surveys, supplier audits and organisational incident records. Additional extensions may include sensitivity analysis over a broader parameter range, Monte Carlo simulation, Bayesian updating or integration with AI-supported and Big Data-driven cyber-risk monitoring systems.

## Conclusions

The article demonstrates that a methodologically transparent framework for assessing supplier cybersecurity risk can be developed using recognised secondary data sources. The research objective was achieved: a weighted scoring model was constructed, its criteria were justified, the AHP method was applied to derive weights, and an illustrative ranking of supplier categories was produced. The research hypothesis is therefore supported within the scope of the adopted methodological framework, rather than fully verified through empirical validation based on organisation-specific data.

The findings indicate that cyber risk in supply chains can be systematically compared when threat exposure, technical vulnerability and operational impact are integrated into a structured assessment model. The results should, however, be interpreted as a preliminary comparative assessment. They demonstrate how publicly available data and transparent assumptions can be transformed into a supplier-risk

index, but they do not replace supplier audits, expert-panel assessments, real-time threat intelligence or organisation-specific cybersecurity evaluation.

The results also suggest that cybersecurity in supply chains should be considered as a cross-functional governance issue linking security, procurement, logistics and continuity management. Supplier-related cyber incidents increasingly reflect systemic interdependencies rather than isolated events. Consequently, approaches to supplier evaluation that rely solely on formal compliance or cost-based criteria may not fully capture the complexity of cyber-risk exposure.

Finally, the article illustrates a practical research approach to cyber supply chain risk analysis. Useful insights can be generated without proprietary datasets if the research design defines its scope, applies appropriate methods and transparently explains the transformation of source data into analytical results. Future development should focus on expert-panel validation, organisation-specific calibration and integration with dynamic data sources.

## References

Bode, C. and Wagner, S.M., 2015. Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. *Journal of Operations Management*, 36, 215–228. DOI: 10.1016/j.jom.2014.12.004.

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A. and Fallon, M., 2022. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. NIST Special Publication 800-161 Rev. 1. Gaithersburg: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-161r1.

Boyson, S., 2014. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7), 342–353. DOI: 10.1016/j.technovation.2014.02.001.

Christopher, M., 2016. *Logistics & Supply Chain Management*. 5th ed. Harlow: Pearson.

Colicchia, C. and Strozzi, F., 2012. Supply chain risk management: a new methodology for a systematic literature review. *Supply Chain Management: An International Journal*, 17(4), 403–418. DOI: 10.1108/13598541211246558.

ENISA, 2021. *Threat Landscape for Supply Chain Attacks* [online]. European Union Agency for Cybersecurity. Available from: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks [Accessed: 15 May 2026].

ENISA, 2023. *Good Practices for Supply Chain Cybersecurity* [online]. European Union Agency for Cybersecurity. Available from: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity [Accessed: 14 May 2026].

ENISA, 2025. *ENISA Threat Landscape 2025* [online]. European Union Agency for

Cybersecurity. Available from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 [Accessed: 14 May 2026].

Heckmann, I., Comes, T. and Nickel, S., 2015. A critical review on supply chain risk: definition, measure and modelling. *Omega*, 52, 119–132. DOI: 10.1016/j.omega.2014.10.004.

IBM, 2025. *Cost of a Data Breach Report* [online]. IBM Security. Available from: https://www.ibm.com/reports/data-breach [Accessed: 12 May 2026].

Ismayilov, V., Ibragimova, N., Babayev, A., Hasanli, A. and Abbasov, A., 2025. Innovative technologies in the logistics system: digital solution implementation benefits and risks assessment. *Military Logistics Systems*, 63(2), 35–56. DOI: 10.37055/slw/218682.

ISO/IEC, 2022. *ISO/IEC 27005:2022 Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks*. Geneva: International Organisation for Standardization.

Ivanov, D., 2021. Supply chain viability and the COVID-19 pandemic: a conceptual and formal generalization of four major adaptation strategies. *International Journal of Production Research*, 59(12), 3535–3552. DOI: 10.1080/00207543.2021.1890852.

Ivanov, D. and Dolgui, A., 2020. Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. *International Journal of Production Research*, 58(10), 2904–2915. DOI: 10.1080/00207543.2020.1750727.

Jałowiec, T. and Spychalski, M.K., 2025. Military logistics system in a crisis situation. *Military Logistics Systems*, 62(1), 95–112. DOI: 10.37055/slw/211041.

Pettit, T.J., Fiksel, J. and Croxton, K.L., 2010. Ensuring supply chain resilience: development of a conceptual framework. *Journal of Business Logistics*, 31(1), 1–21. DOI: 10.1002/j.2158-1592.2010.tb00125.x.

Saaty, T.L., 1987. The analytic hierarchy process — what it is and how it is used. *Mathematical Modelling*, 9(3–5), 161–176. DOI: 10.1016/0270-0255(87)90473-8.

Saaty, T.L., 2008. Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, 1(1), 83–98. DOI: 10.1504/IJSSCI.2008.017590.

Sheffi, Y., 2005. *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. Cambridge, MA: MIT Press.

Tang, C.S., 2006. Perspectives in supply chain risk management. *International Journal of Production Economics*, 103(2), 451–488. DOI: 10.1016/j.ijpe.2005.12.006.

Verizon, 2025. *Data Breach Investigations Report* [online]. Verizon. Available from: https://www.verizon.com/business/resources/reports/dbir/ [Accessed: 14 May 2026].