DIGITAL TRANSFORMATION AND ADMINISTRATION INNOVATION

Citation: Salimi Beni, R. (2027). Dynamic Cyber Risk Assessment for Industrial Automation: Integrating Digital Governance and Predictive Analytics. *Digital Transformation and Administration Innovation,* 5(4), 1-17.

Received date: 2026-07-31 Revised date: 2026-11-12 Accepted date: 2026-11-19 Initial Published date: 2026-11-23 Final Published date: 2027-07-01

Dynamic Cyber Risk Assessment for Industrial Automation: Integrating Digital Governance and Predictive Analytics

Reza Salimi Beni[1]*

1. Master of Science in Information Technology Management, Specialization in Advanced Information Systems, Islamic Azad University, Electronic Campus, Tehran, Iran

*Correspondence: rezasalimi1977@gmail.com

Abstract

This study aimed to develop and empirically evaluate a dynamic cyber risk assessment framework for industrial automation by integrating technical risk indicators, digital governance capability, security control effectiveness, and predictive analytics. A quantitative, applied, longitudinal predictive design was conducted among 278 professionals working in cybersecurity, industrial automation, operational technology, information technology governance, and cyber risk management in Tehran, Iran. Data were collected using a validated multidimensional questionnaire and structured operational cybersecurity indicators obtained from industrial monitoring, vulnerability assessment, incident, and security information systems. The measurement model was assessed using confirmatory factor analysis, Cronbach's alpha, composite reliability, and average variance extracted. Relationships among study variables were examined using correlation and multivariate regression analyses. Predictive performance was evaluated using logistic regression, random forest, gradient boosting, and extreme gradient boosting models, with out-of-sample assessment based on accuracy, precision, recall, F1 score, sensitivity, specificity, area under the receiver operating characteristic curve, and Brier score. Dynamic cyber risk was positively associated with industrial automation vulnerability ($r = 0.69$, $p < .001$) and cyber threat exposure ($r = 0.63$, $p < .001$), and negatively associated with digital governance capability ($r = -0.57$, $p < .001$), security control effectiveness ($r = -0.62$, $p < .001$), and predictive analytics capability ($r = -0.49$, $p < .001$). The regression model explained 68.4% of the variance in dynamic cyber risk ($R^2 = 0.684$, $p < .001$). Industrial automation vulnerability was the strongest positive predictor ($\beta = 0.329$, $p < .001$), while security control effectiveness was the strongest negative predictor ($\beta = -0.222$, $p < .001$). Extreme gradient boosting achieved the best predictive performance, with accuracy = 0.889, F1 = 0.874, and AUC = 0.944. The full integrated model increased AUC from 0.873 to 0.944 compared with the technical-only model. Dynamic cyber risk assessment in industrial automation is substantially improved when technical vulnerabilities and threat exposure are evaluated alongside digital governance, security controls, and predictive analytics, demonstrating that integrated machine-learning models provide a more accurate and actionable representation of evolving cyber risk than conventional technical-only approaches.

Keywords: industrial automation; cyber risk assessment; digital governance; predictive analytics; cybersecurity; operational technology; machine learning; cyber resilience

1. Introduction

The accelerating digitalization of industrial production has transformed industrial automation from a largely isolated operational domain into a highly interconnected cyber-physical ecosystem in which operational technology, information

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

technology, cloud platforms, industrial Internet of Things devices, intelligent sensors, supervisory control systems, and data-driven decision platforms increasingly interact in real time. This transformation has substantially improved productivity, process visibility, flexibility, predictive maintenance, and resource optimization, but it has simultaneously expanded the cyberattack surface and created new dependencies between digital infrastructure and physical processes. In industrial environments, cybersecurity incidents are not limited to confidentiality breaches or information loss; they can interrupt production, manipulate process parameters, degrade equipment performance, compromise worker safety, disrupt supply chains, and generate cascading operational and financial consequences. Consequently, cyber risk assessment has become an essential component of industrial governance rather than merely a technical function delegated to information security teams. Recent scholarship increasingly emphasizes the need to conceptualize cybersecurity as an integrated managerial, technological, and governance challenge that requires coordinated risk identification, monitoring, prediction, mitigation, and accountability across organizational levels (Kamuangu, 2025; Mhlanga, 2026; Rananga & Venter, 2026; Zulfigarzada et al., 2026). Within this context, industrial automation presents a particularly demanding risk environment because operational systems must maintain high availability and continuity while accommodating increasingly sophisticated digital connectivity and analytical capabilities.

Traditional cyber risk assessment approaches have generally relied on periodic audits, vulnerability inventories, qualitative risk matrices, compliance checklists, historical incident records, and static probability-impact evaluations. Although these approaches remain useful for establishing baseline risk profiles, they are frequently insufficient for environments in which vulnerability conditions, threat intensity, system configurations, operational dependencies, and attacker behavior change continuously. A vulnerability considered moderate at one point in time may become critical when combined with a newly disclosed exploit, altered network configuration, remote-access exposure, or a change in the criticality of the affected asset. Similarly, organizations with comparable technical vulnerabilities may face substantially different levels of actual risk depending on their monitoring capacity, incident response maturity, decision structures, security culture, and ability to interpret emerging threat signals. The growing complexity of digital risk has therefore motivated a shift from static assessment toward continuous, adaptive, and predictive approaches capable of incorporating rapidly changing operational information (Paramesha et al., 2024; Pendey, 2023; Rath et al., 2025; Vegas & Llamas, 2024). Such a transition is particularly important in industrial automation, where delayed recognition of deteriorating cyber conditions can allow an apparently localized technical weakness to evolve into a major operational disruption.

Industrial automation environments are structurally different from conventional enterprise information systems. They commonly incorporate programmable logic controllers, supervisory control and data acquisition systems, distributed control systems, industrial communication protocols, human-machine interfaces, engineering workstations, remote maintenance connections, and increasingly, cloud-enabled analytical services and edge devices. Many of these systems were originally designed for reliability and deterministic operation rather than exposure to contemporary cyber threats. Legacy devices, long equipment life cycles, proprietary protocols, limited patching opportunities, inadequate segmentation, insecure authentication mechanisms, and vendor-dependent maintenance arrangements can therefore create persistent vulnerabilities. Furthermore, the convergence of IT and operational technology introduces bidirectional dependencies in which compromises originating in conventional enterprise networks can propagate toward industrial assets and vice versa. Research on digital infrastructure and cybersecurity increasingly recognizes that organizational exposure results from interconnected vulnerabilities rather than isolated technical defects (Akhtar, 2026; Chalyi et al., 2026; Kampourakis et al., 2026; Karras et al., 2025; Rahman et al., 2024). This interconnectedness makes cyber risk dynamic by nature because the severity of a threat depends not only on the existence of a vulnerability but also on network topology, asset criticality, current security controls, adversarial activity, organizational preparedness, and the operational consequences associated with compromise.

At the same time, the growing adoption of artificial intelligence, advanced analytics, automated decision systems, and real-time monitoring has created new opportunities for strengthening industrial cybersecurity. Predictive analytics can process large volumes of historical and streaming data to identify patterns that may precede adverse events, distinguish normal operational behavior from emerging anomalies, prioritize vulnerabilities according to contextual risk, and support earlier intervention. Machine-learning techniques such as random forests, gradient boosting, anomaly-detection models, and ensemble methods can identify nonlinear relationships that conventional risk scoring may fail to capture. These techniques are particularly relevant when risk emerges through interactions among multiple weak signals rather than a single decisive indicator. Contemporary

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

work on predictive systems increasingly emphasizes data integration, automated pattern recognition, adaptive modeling, and real-time intelligence as critical elements of proactive risk management (Almotawkel et al., 2026; Lou et al., 2025; Olaore & Alkhwaldi, 2026; Sufi & Alsulami, 2025; Thapaliya & Bokani, 2024). However, predictive capability should not be interpreted merely as a technical extension of cybersecurity monitoring. Its effectiveness depends heavily on data quality, organizational readiness, model governance, transparency, managerial interpretation, and the capacity to translate analytical outputs into timely operational responses.

This requirement brings digital governance to the center of dynamic cyber risk assessment. Digital governance encompasses the structures, policies, responsibilities, decision rights, accountability mechanisms, oversight arrangements, standards, and coordination processes through which organizations direct and control the use of digital technologies. In industrial environments, effective governance is particularly important because cybersecurity responsibilities are distributed across executive management, IT departments, operational technology teams, engineering units, vendors, risk managers, compliance functions, and frontline operators. Fragmented responsibilities can produce gaps in ownership, inconsistent priorities, delayed remediation, incomplete visibility, and conflicting interpretations of acceptable risk. Strong digital governance can reduce these deficiencies by clarifying authority, establishing accountability, integrating IT and OT decision-making, formalizing risk escalation, ensuring data stewardship, strengthening third-party oversight, and embedding cyber risk into broader organizational decision processes (Harrath et al., 2025; Ibokette et al., 2024; Liang & WeiweiSun, 2025; Mızrak, 2024; Olabanji et al., 2024). Accordingly, the quality of governance may substantially alter the practical significance of technical vulnerabilities: the same technical weakness may present far greater residual risk in an organization with weak oversight and fragmented response mechanisms than in an organization with mature governance and coordinated controls.

The integration of governance into cyber risk models is also important because conventional technical indicators often provide an incomplete picture of organizational exposure. Vulnerability severity, intrusion alerts, failed authentication attempts, abnormal traffic patterns, configuration deviations, malware detections, and patching delays can reveal important aspects of technical risk, but they do not fully indicate whether an organization is capable of interpreting and responding to those signals. Governance maturity, security-control effectiveness, incident preparedness, cyber resilience, data quality, and analytical capability can moderate the translation of technical exposure into actual operational consequences. A dynamic model should therefore distinguish between inherent technical risk and the residual risk that remains after considering governance and organizational control capacity. This perspective is consistent with broader developments in cybersecurity and enterprise risk research, which increasingly treat resilience, governance, compliance, strategic decision-making, and operational preparedness as complementary rather than separate dimensions (Chahal, 2023; Familoni, 2024; Mohammed, 2024; Onih et al., 2024; Shoetan et al., 2024). Integrating these dimensions can produce a more realistic assessment of cyber risk because it captures both the likelihood of adverse events and the organization's ability to prevent, absorb, respond to, and recover from them.

Another major challenge concerns the temporal nature of cyber risk. Static frameworks typically assign risk scores that remain unchanged until the next formal assessment, even though the underlying environment may evolve within hours or minutes. In industrial automation, risk can increase abruptly following a new vulnerability disclosure, abnormal access behavior, a change in asset connectivity, the appearance of malicious traffic, a third-party compromise, or a deterioration in security-control effectiveness. Conversely, risk can decline following remediation, improved segmentation, stronger authentication, enhanced monitoring, or more effective governance intervention. Dynamic assessment therefore requires mechanisms capable of updating risk scores as new evidence becomes available. This involves combining historical records with current telemetry, contextualizing technical indicators according to asset criticality, and incorporating organizational variables that influence the effectiveness of mitigation. Recent research on data-intensive risk systems has increasingly stressed continuous monitoring, scenario sensitivity, early warning, and adaptive risk estimation (Andrei & Scarlat, 2024; Islam, 2024; Manowska & Syta, 2026; Picano, 2025; Pochmara & Świetlicka, 2024). For industrial organizations, such an approach offers the possibility of shifting cybersecurity management from periodic diagnosis toward continuous anticipation and prioritization.

Predictive modeling is especially valuable in this context because cyber risk is often characterized by complex interactions, nonlinear effects, and imbalanced outcome distributions. Linear or rule-based approaches may perform adequately when relationships are simple and stable, but they may be less effective when combinations of vulnerabilities, governance

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

weaknesses, anomalous events, and operational conditions jointly determine the probability of elevated risk. Ensemble machine-learning methods can accommodate interactions among heterogeneous predictors and identify complex thresholds beyond which risk increases rapidly. At the same time, predictive performance alone is insufficient for organizational adoption. Industrial decision-makers require models that are interpretable enough to support risk prioritization, resource allocation, auditability, and accountability. Feature-importance techniques and explainable artificial intelligence approaches can therefore complement predictive algorithms by showing which technical and governance variables most strongly contribute to estimated risk (Dayakar Babu Kancherla Prof. Nishant, 2024; Eskandarany, 2024; Gupta, 2024; Karras et al., 2025). The combination of predictive accuracy and interpretability is particularly relevant for industrial settings, where security recommendations may affect production schedules, equipment availability, maintenance activities, and safety-sensitive processes.

The need for interpretability also reinforces the importance of governance in the use of predictive analytics itself. Models that generate risk scores without clear accountability, validation procedures, data-quality controls, or decision protocols may create a false sense of precision. Digital governance should therefore address not only cybersecurity controls but also the governance of analytical systems used to evaluate cybersecurity. This includes defining ownership of predictive models, determining acceptable data sources, validating model performance, monitoring drift, documenting decision rules, controlling access to sensitive operational data, and ensuring that automated recommendations do not bypass appropriate human oversight. The broader literature on digital transformation increasingly highlights the importance of balancing technological innovation with transparency, responsibility, organizational alignment, and institutional control (Antonio João Gonçalves de et al., 2023; Kamuangu, 2025; Liang & WeiweiSun, 2025; Mhlanga, 2026). In cyber risk assessment, this balance is particularly consequential because poorly governed analytics may misclassify critical threats, over-prioritize benign anomalies, or obscure the organizational factors that contribute to vulnerability.

A further issue is that many cybersecurity frameworks conceptually separate governance, technical defense, and analytics even though these domains interact continuously in practice. Governance determines which risks receive attention, how quickly vulnerabilities are remediated, which controls are funded, how responsibilities are distributed, and how incident information is escalated. Technical controls generate and constrain the operational signals from which risk is estimated. Predictive analytics transform these signals into probabilistic assessments and prioritization mechanisms. Cyber resilience determines whether the organization can maintain or rapidly restore critical functions when preventive measures fail. Treating these dimensions independently may therefore obscure their cumulative contribution to actual cyber risk. A more integrated framework can capture the interaction between threat exposure, technical vulnerability, protective controls, governance capability, and analytical maturity, thereby reflecting cyber risk as an emergent organizational condition rather than a purely technological metric (Akhtar, 2026; Harrath et al., 2025; Rananga & Venter, 2026; Rath et al., 2025; Vegas & Llamas, 2024). This integrated perspective is especially necessary in automation-intensive industries, where the boundary between digital systems and physical operations is increasingly difficult to separate.

Cyber resilience further extends the logic of dynamic assessment by recognizing that prevention alone cannot eliminate industrial cyber risk. Organizations must also be capable of detecting attacks rapidly, limiting propagation, preserving critical functions, recovering affected systems, and learning from incidents. Resilience therefore depends on a combination of technical redundancy, incident-response capability, governance coordination, workforce preparedness, communication mechanisms, and continuous learning. Predictive analytics can contribute to resilience by identifying deteriorating conditions before they produce severe disruption, while digital governance can ensure that warnings lead to timely and coordinated intervention. Studies addressing emerging approaches to cybersecurity and organizational continuity increasingly emphasize preparedness, adaptive response, strategic risk governance, and recovery capabilities as central components of effective cyber defense (Almotawkel et al., 2026; Familoni, 2024; Mızrak, 2024; Sufi & Alsulami, 2025; Thapaliya & Bokani, 2024). From this standpoint, dynamic risk assessment is not merely a mechanism for assigning a score but a decision-support process connecting detection, prediction, governance, response, and organizational resilience.

Despite these advances, an important research gap remains in the empirical integration of digital governance variables and predictive analytics within a unified dynamic cyber risk assessment framework specifically designed for industrial automation. Much existing research emphasizes either technical cybersecurity, enterprise governance, artificial intelligence, vulnerability

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

prediction, or resilience in relative isolation. Fewer studies empirically examine whether adding governance capability to technical risk indicators improves predictive discrimination, calibration, and explanatory value, particularly in operational technology environments. Moreover, the practical value of predictive analytics depends on demonstrating that integrated models outperform conventional assessments based primarily on technical exposure. This requires systematic comparison of models, evaluation of out-of-sample performance, and identification of the relative importance of governance, controls, vulnerabilities, and threat exposure. Current developments across cybersecurity, digital risk management, and predictive modeling collectively point toward the need for such integrative approaches (Gupta, 2024; Lou et al., 2025; Manowska & Syta, 2026; Olaore & Alkhwaldi, 2026; Paramesha et al., 2024; Picano, 2025; Pochmara & Świetlicka, 2024).

The industrial context of Tehran provides a relevant empirical environment for examining these relationships because organizations operating complex automation infrastructures increasingly depend on interconnected digital technologies while simultaneously managing legacy systems, heterogeneous security architectures, governance constraints, and varying levels of analytical maturity. Evaluating cyber risk within such an environment permits simultaneous examination of technological vulnerabilities and organizational capabilities. Furthermore, integrating survey-based governance measures with operational cyber indicators can provide a broader perspective than approaches based exclusively on self-reported perceptions or technical telemetry. This combined analytical logic is consistent with the growing recognition that effective cybersecurity assessment should incorporate technological, managerial, behavioral, and organizational dimensions (Chalyi et al., 2026; Ibokette et al., 2024; Mohammed, 2024; Onih et al., 2024; Rahman et al., 2024; Shoetan et al., 2024; Zulfigarzada et al., 2026). It also enables direct examination of whether stronger governance and predictive capability meaningfully reduce estimated cyber risk after accounting for vulnerability and threat exposure.

Taken together, the contemporary industrial cybersecurity landscape demonstrates that risk is increasingly dynamic, multidimensional, and dependent on the interaction between technological exposure and organizational capacity. Static assessment models remain useful for baseline documentation but are poorly suited to environments characterized by continuous connectivity, evolving attack techniques, changing vulnerabilities, and time-sensitive operational consequences. Predictive analytics provides the computational capacity to identify emerging risk patterns, while digital governance provides the institutional capacity to ensure that those predictions are interpreted, prioritized, and translated into effective action. Integrating these perspectives can therefore strengthen both the technical accuracy and managerial relevance of cyber risk assessment. The emerging literature on digital security, artificial intelligence, governance, automation, and organizational resilience consistently underscores the importance of adaptive and integrated approaches to contemporary cyber risk (Andrei & Scarlat, 2024; Antonio João Gonçalves de et al., 2023; Chahal, 2023; Eskandarany, 2024; Islam, 2024; Kampourakis et al., 2026; Karras et al., 2025; Liang & WeiweiSun, 2025; Mhlanga, 2026; Olabanji et al., 2024). Accordingly, the aim of the present study was to develop and empirically evaluate a dynamic cyber risk assessment framework for industrial automation by integrating technical risk indicators, digital governance capability, security control effectiveness, and predictive analytics to improve the identification and prediction of elevated cyber risk conditions.

2. Methods and Materials

This study employed a quantitative, applied, longitudinal predictive design to develop and evaluate a dynamic cyber risk assessment framework for industrial automation environments by integrating digital governance indicators with operational cybersecurity data and predictive analytics. The study population consisted of cybersecurity specialists, industrial automation engineers, information technology managers, operational technology professionals, digital governance specialists, risk managers, and technical managers employed in industrial organizations and automation-related companies located in Tehran, Iran. Participants were recruited from manufacturing companies, process industries, energy-related organizations, industrial automation service providers, and organizations operating integrated information technology and operational technology infrastructures. A purposive stratified sampling approach was adopted to ensure adequate representation of professionals involved in cybersecurity governance, industrial control systems, automation engineering, risk management, and technology management. Eligibility criteria included having at least three years of professional experience in industrial automation, cybersecurity, operational technology, information technology governance, or cyber risk management; direct involvement in

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

the management, operation, monitoring, security, or governance of industrial automation systems; and familiarity with at least one industrial control environment such as Supervisory Control and Data Acquisition systems, Distributed Control Systems, Programmable Logic Controllers, Industrial Internet of Things platforms, or integrated IT/OT networks. Individuals whose professional activities were exclusively administrative and who had no direct involvement in cybersecurity, digital governance, automation, or technology risk management were excluded. A total of 318 eligible professionals were initially invited to participate, of whom 291 completed the research instruments. Following data screening, 13 questionnaires were excluded because of substantial missing data, patterned responses, or failure to satisfy the predefined data-quality criteria, resulting in a final analytical sample of 278 participants. Data collection was conducted in Tehran over a six-month period. To incorporate the dynamic dimension of cyber risk, organizational cybersecurity and automation-related operational indicators were also collected at repeated intervals for participating organizational units, thereby allowing changes in vulnerability exposure, security-event frequency, governance performance, control effectiveness, and operational anomalies to be incorporated into the predictive model. Participation was voluntary, respondents were informed of the purpose and procedures of the study, confidentiality of organizational and individual information was maintained, and all analytical data were anonymized before statistical and computational processing.

Data were collected using an integrated cyber risk assessment instrument specifically constructed for industrial automation environments and a standardized data-extraction protocol for operational cybersecurity indicators. The questionnaire consisted of sections measuring digital governance capability, cybersecurity governance, industrial automation vulnerability, cyber threat exposure, security control effectiveness, organizational cyber resilience, incident preparedness, data governance, accountability mechanisms, risk monitoring capability, and predictive analytics maturity. Digital governance was operationalized through dimensions covering governance structure, definition of cybersecurity responsibilities, executive oversight, policy formalization, regulatory compliance, data stewardship, auditability, accountability, interdepartmental coordination, IT/OT governance integration, third-party governance, and continuous risk oversight. Industrial cyber risk indicators included exposure of critical automation assets, network segmentation weaknesses, insecure remote access, obsolete or unsupported components, patching delays, access-control deficiencies, abnormal network activities, unauthorized configuration changes, vulnerability severity, frequency of security alerts, previous cyber incidents, recovery capability, and the criticality of affected operational assets. Predictive analytics capability was assessed through the availability and integration of historical security data, real-time monitoring, automated event analysis, anomaly detection, predictive modeling, threat intelligence integration, model-based risk prioritization, and the organizational use of predictive outputs in cybersecurity decision-making. Questionnaire items were measured on a five-point Likert scale ranging from 1, representing very low or strongly disagree, to 5, representing very high or strongly agree, depending on the wording of the construct. The initial item pool was developed through a review of industrial cybersecurity, operational technology risk management, digital governance, and predictive risk assessment literature and was subsequently evaluated by a panel of 12 specialists in cybersecurity, industrial automation, information systems governance, and quantitative modeling. Content validity was examined in terms of relevance, clarity, comprehensiveness, and consistency with the conceptual definitions of the constructs, and items considered ambiguous or redundant were revised or removed prior to the main data collection. A pilot study involving 30 professionals with characteristics comparable to those of the main sample was conducted to assess comprehensibility, completion time, preliminary reliability, and instrument functionality. Internal consistency was subsequently evaluated using Cronbach's alpha and composite reliability, while convergent validity was assessed through standardized factor loadings and average variance extracted. Discriminant validity was examined by comparing relationships among latent constructs and by evaluating whether conceptually distinct dimensions demonstrated adequate empirical separation. In addition to questionnaire information, a structured operational data form was used to obtain non-identifying cybersecurity indicators from available security information and event management systems, intrusion detection systems, vulnerability assessment reports, industrial control monitoring platforms, network monitoring systems, maintenance records, and cybersecurity incident reports. The operational variables included the number and severity of detected vulnerabilities, failed authentication attempts, anomalous communication patterns, unusual protocol activity, unauthorized access events, malware or intrusion alerts, configuration deviations, patching delays, asset criticality, system downtime associated with security events, and frequency and severity of previously recorded incidents. These indicators were normalized before modeling and were combined with digital governance measures to produce

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

a multidimensional representation of cyber risk that reflected not only existing technical vulnerabilities but also the organizational capacity to govern, anticipate, detect, respond to, and recover from emerging cybersecurity threats.

Data analysis was performed through an integrated statistical and machine-learning procedure designed to construct and validate a dynamic cyber risk prediction model for industrial automation environments. Initially, the dataset was examined for incomplete observations, duplicate records, inconsistent responses, extreme values, and anomalous measurement patterns. Missing values were evaluated according to their extent and distribution, and records exceeding the predefined missing-data threshold were removed, whereas limited missing observations were treated using appropriate imputation procedures. Descriptive statistics, including mean, standard deviation, minimum, maximum, frequency, and distributional characteristics, were calculated to describe the research variables and evaluate the general structure of the data. Measurement quality was assessed using confirmatory factor analysis, standardized factor loadings, Cronbach's alpha, composite reliability, and average variance extracted. Correlations among digital governance, technical cyber risk indicators, predictive analytics capability, cybersecurity resilience, and the overall dynamic risk measure were examined before predictive modeling. For development of the dynamic risk assessment model, the dataset was divided into training and testing subsets while preserving the temporal ordering of operational observations to prevent information leakage from future observations into earlier prediction periods. A combination of conventional and machine-learning models was evaluated, including logistic regression as a baseline statistical model, random forest, gradient-boosted decision trees, and extreme gradient boosting. Where sequential operational observations were available, lagged risk variables and moving-window indicators were generated to represent short-term changes in threat intensity, vulnerability conditions, and security-control performance. Predictor variables incorporated technical exposure indicators together with digital governance scores so that the estimated risk level reflected both the probability of a cyber event and the organization's governance capacity to mitigate its consequences. Hyperparameters were optimized using cross-validation performed exclusively within the training data, and predictive performance was evaluated on unseen test observations using accuracy, precision, recall, F1 score, sensitivity, specificity, area under the receiver operating characteristic curve, and, where continuous risk scores were estimated, mean absolute error and root mean squared error. Model calibration was also examined to determine the consistency between predicted risk probabilities and observed cyber risk outcomes. The relative contribution of individual predictors was evaluated through feature-importance analysis and SHAP-based interpretation, enabling identification of the technical and governance factors that most strongly influenced predicted cyber risk. The final dynamic cyber risk score was computed by integrating model-estimated incident probability, vulnerability severity, asset criticality, threat exposure, security-control effectiveness, and digital governance capability into a continuously updateable risk index. Higher values represented greater predicted cyber risk, whereas improvements in governance quality, control effectiveness, monitoring capability, and organizational resilience reduced the adjusted risk estimate. Sensitivity analyses were conducted by comparing models containing only technical cybersecurity variables with models incorporating both technical indicators and digital governance variables; improvement in predictive accuracy, discrimination, and calibration was interpreted as evidence of the incremental contribution of governance information to cyber risk assessment. All hypothesis tests were evaluated at a significance level of $p < .05$, while predictive performance was interpreted primarily on the basis of out-of-sample validation rather than statistical significance alone. Statistical analyses were conducted using SPSS and AMOS for preliminary statistical and measurement analyses, while Python-based analytical libraries were used for machine-learning model development, validation, interpretation, and dynamic cyber risk estimation.

3. Findings and Results

The final analytical sample consisted of 278 professionals working in industrial automation, cybersecurity, operational technology, information technology governance, and cyber risk management in Tehran. Of the participants, 202 individuals (72.7%) were male and 76 (27.3%) were female. The mean age of the respondents was 39.62 years (SD = 7.84), with participants ranging from 27 to 58 years of age. In terms of educational attainment, 46 participants (16.5%) held a bachelor's degree, 174 (62.6%) held a master's degree, and 58 (20.9%) held a doctoral degree or equivalent advanced professional qualification. Professional experience averaged 11.74 years (SD = 5.91), and 69 participants (24.8%) reported between 3 and 7 years of relevant experience, 111 (39.9%) reported between 8 and 12 years, and 98 (35.3%) had more than 12 years of professional experience. Regarding professional specialization, 66 participants (23.7%) worked primarily in cybersecurity and

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

information security, 59 (21.2%) in industrial automation and control engineering, 52 (18.7%) in operational technology and industrial network management, 43 (15.5%) in information technology governance and digital transformation, 34 (12.2%) in enterprise or cyber risk management, and 24 (8.6%) in senior technical or operational management positions. In terms of organizational context, 81 respondents (29.1%) were employed in manufacturing organizations, 59 (21.2%) in process industries, 46 (16.5%) in energy-related organizations, 39 (14.0%) in industrial automation and engineering service companies, 31 (11.2%) in technology-intensive infrastructure organizations, and 22 (7.9%) in other industrial organizations with integrated IT/OT environments. Overall, the demographic and professional composition of the sample demonstrated substantial representation of technically experienced professionals with direct exposure to industrial automation, operational technology, cybersecurity governance, and cyber risk management, providing an appropriate empirical basis for evaluating the proposed dynamic cyber risk assessment framework.

Table 1. Descriptive Statistics, Reliability, and Convergent Validity of the Main Study Constructs

Construct	Mean	SD	Standardized Loading Range	Cronbach's α	Composite Reliability	AVE
Digital Governance Capability	3.61	0.63	0.71–0.87	0.91	0.93	0.62
Cybersecurity Governance	3.55	0.67	0.70–0.86	0.89	0.92	0.59
Industrial Automation Vulnerability	3.34	0.71	0.72–0.88	0.90	0.92	0.61
Cyber Threat Exposure	3.47	0.69	0.73–0.89	0.92	0.94	0.65
Security Control Effectiveness	3.58	0.64	0.69–0.85	0.88	0.91	0.57
Organizational Cyber Resilience	3.49	0.66	0.72–0.90	0.91	0.93	0.63
Incident Preparedness	3.41	0.70	0.70–0.88	0.89	0.92	0.60
Predictive Analytics Capability	3.28	0.73	0.74–0.91	0.93	0.95	0.67
Dynamic Cyber Risk	3.39	0.68	0.75–0.90	0.92	0.94	0.66

As shown in Table 1, the descriptive results indicated moderate to relatively high levels across the organizational and technological constructs examined in the study. Digital governance capability had a mean of 3.61 (SD = 0.63), while cybersecurity governance had a mean of 3.55 (SD = 0.67), indicating that participating organizations generally reported established governance mechanisms, although considerable scope for improvement remained. Security control effectiveness also demonstrated a relatively favorable mean of 3.58 (SD = 0.64), whereas predictive analytics capability yielded the lowest mean among the principal constructs at 3.28 (SD = 0.73). This finding suggested that, despite the presence of conventional cybersecurity and governance mechanisms, the systematic utilization of historical data, real-time analytics, automated anomaly identification, and predictive modeling remained comparatively less developed. Industrial automation vulnerability and cyber threat exposure produced means of 3.34 (SD = 0.71) and 3.47 (SD = 0.69), respectively, indicating a meaningful level of technical exposure within the participating industrial environments. The mean dynamic cyber risk score was 3.39 (SD = 0.68), demonstrating that the sampled environments generally operated under a moderate but non-negligible cyber risk condition. The measurement properties were satisfactory across all constructs. Cronbach's alpha coefficients ranged from 0.88 to 0.93, exceeding the conventional threshold of 0.70 and indicating strong internal consistency. Composite reliability coefficients ranged from 0.91 to 0.95, further supporting the reliability of the latent constructs. Average variance extracted values ranged from 0.57 to 0.67 and therefore exceeded the recommended value of 0.50, confirming satisfactory convergent validity. Standardized factor loadings ranged from 0.69 to 0.91, with the large majority exceeding 0.70. Collectively, these results supported the adequacy of the measurement model and demonstrated that the constructs used in the subsequent structural and predictive analyses represented their underlying theoretical dimensions with acceptable reliability and convergent validity.

Table 2. Correlations Between Digital Governance, Technical Cybersecurity Factors, Predictive Analytics, and Dynamic Cyber Risk

Variable	1	2	3	4	5	6	7
1. Digital Governance Capability	1						
2. Cybersecurity Governance	0.68***	1					
3. Industrial Automation Vulnerability	-0.42***	-0.39***	1				
4. Cyber Threat Exposure	-0.31***	-0.28***	0.57***	1			
5. Security Control Effectiveness	0.61***	0.66***	-0.48***	-0.37***	1		
6. Predictive Analytics Capability	0.59***	0.55***	-0.35***	-0.29***	0.53***	1	
7. Dynamic Cyber Risk	-0.57***	-0.53***	0.69***	0.63***	-0.62***	-0.49***	1

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Table 2 presents the bivariate relationships among the principal governance, cybersecurity, technological, and risk variables. Dynamic cyber risk was positively and strongly associated with industrial automation vulnerability ($r = 0.69$, $p < .001$) and cyber threat exposure ($r = 0.63$, $p < .001$), indicating that organizations characterized by greater technical weaknesses, insecure configurations, delayed patching, exposed critical assets, anomalous network activity, and more frequent threat indicators experienced substantially higher levels of overall cyber risk. In contrast, dynamic cyber risk was negatively correlated with digital governance capability ($r = -0.57$, $p < .001$), cybersecurity governance ($r = -0.53$, $p < .001$), security control effectiveness ($r = -0.62$, $p < .001$), and predictive analytics capability ($r = -0.49$, $p < .001$). These findings suggested that organizations with stronger digital governance structures, clearer accountability, better integration of IT and OT governance, more effective technical controls, and greater capacity for predictive monitoring tended to exhibit lower cyber risk. Digital governance capability was itself strongly associated with cybersecurity governance ($r = 0.68$, $p < .001$), security control effectiveness ($r = 0.61$, $p < .001$), and predictive analytics capability ($r = 0.59$, $p < .001$), indicating that governance maturity was closely related to both the strength of existing security mechanisms and the organization's capacity to operationalize predictive analytics. Industrial automation vulnerability was positively correlated with cyber threat exposure ($r = 0.57$, $p < .001$) but negatively associated with security control effectiveness ($r = -0.48$, $p < .001$) and predictive analytics capability ($r = -0.35$, $p < .001$). The pattern of correlations therefore supported the theoretical premise of the proposed framework: technical vulnerability and threat exposure increased dynamic cyber risk, whereas governance maturity, effective controls, and predictive capabilities operated as protective organizational mechanisms. None of the correlations exceeded levels that would ordinarily indicate severe multicollinearity, allowing the variables to be entered simultaneously into subsequent multivariate and predictive models.

Table 3. Multivariate Predictors of Dynamic Cyber Risk

Predictor	B	SE	Standardized β	t	p	VIF
Digital Governance Capability	-0.218	0.048	-0.202	-4.54	<.001	2.01
Cybersecurity Governance	-0.143	0.051	-0.141	-2.80	.005	2.18
Industrial Automation Vulnerability	0.314	0.041	0.329	7.66	<.001	1.72
Cyber Threat Exposure	0.261	0.043	0.264	6.07	<.001	1.58
Security Control Effectiveness	-0.237	0.049	-0.222	-4.84	<.001	2.11
Predictive Analytics Capability	-0.156	0.040	-0.168	-3.90	<.001	1.65

Model Statistic	Value
R^2	0.684
Adjusted R^2	0.677
F	97.79
Model p	<.001
Durbin–Watson	1.96

The multivariate regression results presented in Table 3 demonstrated that the combination of governance, technical exposure, control effectiveness, and predictive analytics variables explained a substantial proportion of the variance in dynamic cyber risk. The overall model was statistically significant, $F = 97.79$, $p < .001$, with an R^2 of 0.684 and an adjusted R^2 of 0.677, indicating that approximately 68.4% of the variance in dynamic cyber risk was explained by the six predictors included in the model. Industrial automation vulnerability emerged as the strongest positive predictor of dynamic cyber risk ($\beta = 0.329$, $t = 7.66$, $p < .001$), demonstrating that increases in technical vulnerabilities, insecure industrial assets, weak segmentation, patching delays, legacy components, and configuration weaknesses were associated with pronounced increases in overall risk. Cyber threat exposure was also a strong positive predictor ($\beta = 0.264$, $t = 6.07$, $p < .001$), confirming that more frequent and severe threat indicators directly increased the estimated cyber risk level. Among the protective factors, security control effectiveness exerted the strongest negative effect ($\beta = -0.222$, $t = -4.84$, $p < .001$), indicating that effective access control, network segmentation, monitoring, incident detection, configuration management, and defensive mechanisms significantly reduced risk. Digital governance capability also had a significant negative effect on dynamic cyber risk ($\beta = -0.202$, $t = -4.54$, $p < .001$), demonstrating that governance structures, managerial oversight, accountability, data stewardship, compliance, and integrated IT/OT decision-making provided a meaningful reduction in overall cyber exposure. Predictive analytics capability independently reduced cyber risk ($\beta = -0.168$, $t = -3.90$, $p < .001$), supporting the proposition that organizations capable of identifying emerging anomalies, generating early-warning signals, and using historical and real-time data to anticipate adverse cyber events were better positioned to manage evolving risks. Cybersecurity governance additionally demonstrated a significant

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

negative relationship with cyber risk (β = -0.141, t = -2.80, p = .005). Variance inflation factor values ranged from 1.58 to 2.18, indicating that multicollinearity was not problematic, while the Durbin–Watson statistic of 1.96 supported independence of residuals. The overall pattern of results confirmed that dynamic cyber risk in industrial automation environments cannot be adequately explained by technical vulnerabilities alone; rather, governance quality, security control effectiveness, and predictive analytical capability contribute independently and materially to risk reduction.

Table 4. Predictive Performance of Cyber Risk Classification Models

Model	Accuracy	Precision	Recall	F1 Score	Sensitivity	Specificity	AUC
Logistic Regression	0.794	0.781	0.758	0.769	0.758	0.821	0.842
Random Forest	0.849	0.842	0.823	0.832	0.823	0.870	0.907
Gradient Boosting	0.867	0.858	0.844	0.851	0.844	0.885	0.925
Extreme Gradient Boosting	0.889	0.881	0.867	0.874	0.867	0.906	0.944

Table 4 compares the out-of-sample predictive performance of the four classification algorithms evaluated for identifying elevated cyber risk conditions in industrial automation environments. All machine-learning models outperformed the conventional logistic regression benchmark across the principal classification criteria. Logistic regression achieved an accuracy of 0.794 and an AUC of 0.842, indicating acceptable but comparatively limited discrimination between lower-risk and elevated-risk observations. Random forest improved accuracy to 0.849 and achieved an AUC of 0.907, suggesting that nonlinear interactions and variable combinations contributed meaningfully to risk classification. Gradient boosting produced further improvement, with an accuracy of 0.867, F1 score of 0.851, and AUC of 0.925. The best overall performance was observed for the extreme gradient boosting model, which achieved an accuracy of 0.889, precision of 0.881, recall of 0.867, F1 score of 0.874, sensitivity of 0.867, specificity of 0.906, and AUC of 0.944. The combination of high sensitivity and specificity demonstrated that the model was capable of identifying a substantial proportion of genuinely elevated-risk observations without generating an excessive number of false-positive classifications. The AUC value of 0.944 indicated excellent discrimination and showed that the model could distinguish between elevated and lower cyber risk conditions with a high degree of consistency. The improvement from logistic regression to extreme gradient boosting was particularly notable because it demonstrated that cyber risk was influenced by nonlinear and interaction effects that were not fully represented by a conventional linear classification model. The results therefore supported the use of advanced predictive analytics for dynamic cyber risk assessment, particularly when technical, operational, and governance variables were considered jointly.

Table 5. Incremental Predictive Value of Digital Governance and Predictive Analytics in the Extreme Gradient Boosting Model

Model Configuration	Accuracy	F1 Score	AUC	Brier Score	Improvement in AUC
Technical Risk Indicators Only	0.818	0.801	0.873	0.164	—
Technical Indicators + Security Controls	0.846	0.829	0.901	0.143	+0.028
Technical Indicators + Digital Governance	0.864	0.847	0.921	0.129	+0.048
Full Integrated Model	0.889	0.874	0.944	0.107	+0.071

Table 5 evaluates the incremental predictive contribution of governance and predictive analytics by comparing nested configurations of the best-performing extreme gradient boosting model. The model using only technical risk indicators, including vulnerability severity, threat exposure, asset criticality, abnormal activities, patching delays, and security-event frequency, achieved an accuracy of 0.818 and an AUC of 0.873. Adding security control effectiveness increased the AUC to 0.901 and reduced the Brier score from 0.164 to 0.143, indicating improvements in both discrimination and probability calibration. When digital governance variables were incorporated alongside technical indicators, predictive performance improved further, with accuracy rising to 0.864 and AUC reaching 0.921. The full integrated model, incorporating technical risk indicators, security controls, digital governance, and predictive analytics capability, achieved the strongest overall results, with an accuracy of 0.889, F1 score of 0.874, AUC of 0.944, and Brier score of 0.107. Relative to the technical-only model, the full model improved the AUC by 0.071, representing a substantial increase in discriminatory performance. The progressive decline in the Brier score further demonstrated that the integrated model not only classified observations more accurately but also generated more reliable risk probabilities. These findings provide direct empirical support for the central premise of the study: dynamic cyber risk assessment becomes substantially more informative when conventional technical indicators are complemented by information concerning governance maturity, security control effectiveness, and predictive analytical

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

capability. In practical terms, the findings indicate that two industrial organizations with similar technical vulnerability profiles may nonetheless exhibit meaningfully different overall cyber risk when their governance quality, organizational preparedness, and capacity to detect emerging threats differ.

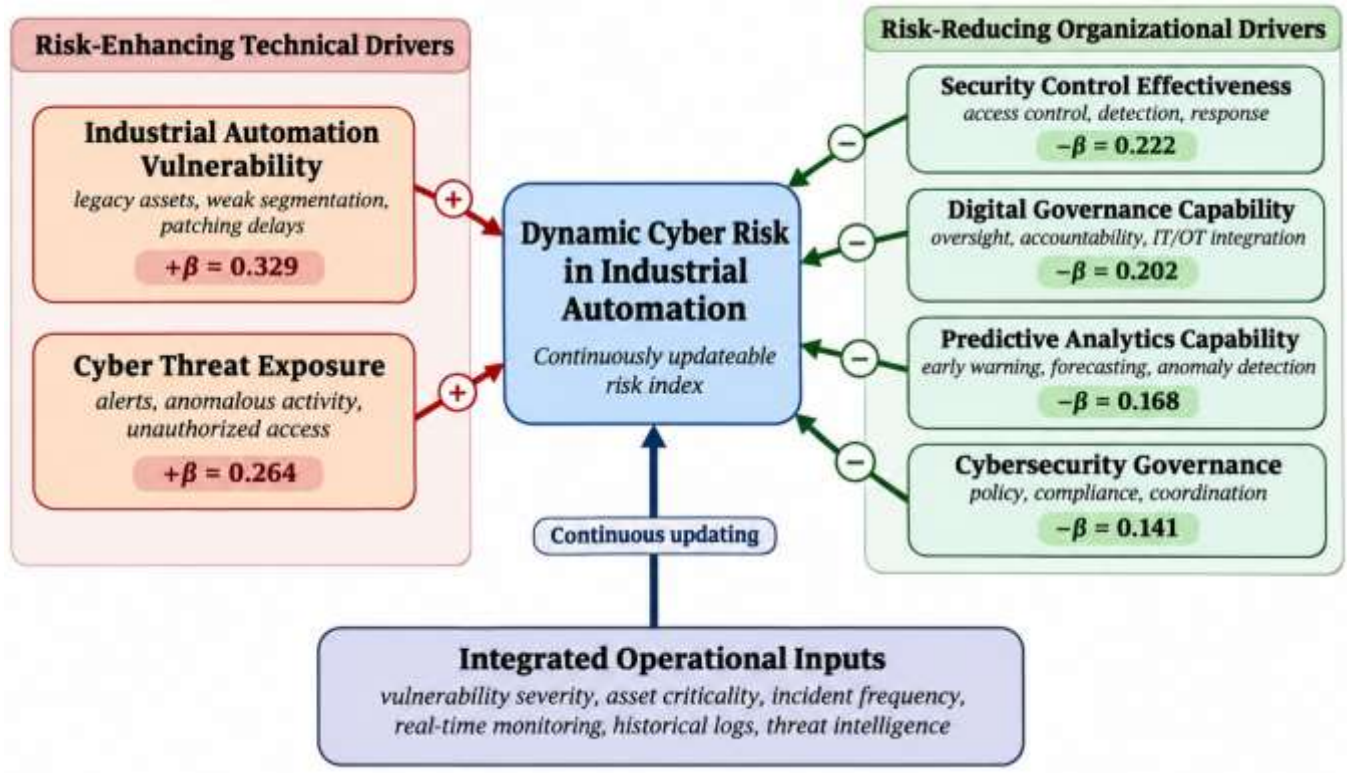


Figure 1. Integrated Predictive Model of Dynamic Cyber Risk in Industrial Automation

Figure 1 illustrates the empirical structure of the proposed dynamic cyber risk assessment model and summarizes the direction and relative importance of the principal factors contributing to predicted cyber risk. The model positions industrial automation vulnerability and cyber threat exposure as the two principal risk-enhancing dimensions, whereas digital governance capability, cybersecurity governance, security control effectiveness, and predictive analytics capability operate as risk-reducing dimensions. Within the predictive framework, industrial automation vulnerability exerted the largest positive contribution to elevated cyber risk, followed by threat exposure, whereas effective security controls and digital governance represented the most influential protective factors. Predictive analytics contributed both directly and indirectly to risk reduction by enabling earlier recognition of abnormal behavior, more accurate prioritization of vulnerabilities, and more timely adjustment of organizational responses. The model therefore conceptualizes cyber risk as a continuously changing outcome produced by the interaction between technical exposure and organizational capacity rather than as a static consequence of vulnerabilities alone. The strongest predictive configuration emerged when real-time and historical technical indicators were integrated with governance and analytical capability variables, demonstrating that dynamic cyber risk assessment should combine operational telemetry with organizational and managerial information. In this framework, increases in threat frequency, asset criticality, vulnerability severity, anomalous activity, and control deficiencies dynamically raise the estimated risk score, whereas stronger governance, effective controls, greater resilience, and predictive capability reduce the adjusted risk estimate. The figure consequently represents the core analytical contribution of the study by demonstrating how cyber risk in industrial automation environments can be continuously updated through the simultaneous consideration of technical, operational, managerial, and predictive information.

4. Discussion and Conclusion

The present study developed and evaluated a dynamic cyber risk assessment framework for industrial automation by integrating technical exposure indicators, digital governance capability, security control effectiveness, and predictive analytics. The findings provide convergent evidence that cyber risk in industrial automation environments is best understood as a

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

multidimensional and continuously evolving condition rather than as a static function of technical vulnerability alone. The descriptive results showed that participating organizations demonstrated moderate to relatively high levels of digital governance, cybersecurity governance, security control effectiveness, organizational cyber resilience, and incident preparedness, while predictive analytics capability was comparatively less developed. At the same time, industrial automation vulnerability and cyber threat exposure remained at meaningful levels, producing a moderate overall dynamic cyber risk profile. This pattern is theoretically significant because it suggests that many organizations may possess formal governance and cybersecurity structures without yet achieving comparable maturity in predictive and anticipatory risk capabilities. Such a gap is consistent with the broader transition in cybersecurity from reactive control toward adaptive, data-driven, and predictive risk management, in which organizations are increasingly required to combine governance maturity with intelligent monitoring and analytical infrastructures (Kamuangu, 2025; Mhlanga, 2026; Rath et al., 2025; Zulfigarzada et al., 2026). The findings therefore indicate that conventional governance and control mechanisms remain important but are not sufficient by themselves to address the velocity and complexity of cyber threats affecting modern industrial automation systems.

The measurement results further supported the internal consistency and construct validity of the framework. All latent constructs demonstrated strong reliability, satisfactory composite reliability, acceptable average variance extracted, and appropriate standardized factor loadings. This finding is important because the proposed framework integrates conceptually distinct but closely related dimensions, including governance, vulnerability, threat exposure, control effectiveness, resilience, preparedness, and predictive capability. The empirical separation of these constructs suggests that dynamic cyber risk is not merely a relabeling of vulnerability severity or cybersecurity maturity but a broader construct produced by the interaction of technical and organizational factors. This multidimensional interpretation aligns with emerging research that emphasizes the need to move beyond narrow technology-centric cybersecurity models and incorporate institutional, managerial, governance, and analytical components into risk assessment (Harrath et al., 2025; Liang & WeiweiSun, 2025; Rananga & Venter, 2026; Shoetan et al., 2024). The satisfactory measurement properties also strengthen the analytical basis for using governance and predictive analytics variables as distinct explanatory components rather than treating them as peripheral contextual characteristics.

The correlation analysis revealed a clear and theoretically coherent pattern. Dynamic cyber risk was positively and strongly related to industrial automation vulnerability and cyber threat exposure, whereas it was negatively associated with digital governance capability, cybersecurity governance, security control effectiveness, and predictive analytics capability. The strongest positive relationship was observed between industrial automation vulnerability and dynamic cyber risk, which indicates that technical weaknesses remain central to the risk structure of industrial environments. Legacy assets, inadequate segmentation, delayed patching, weak authentication, insecure remote access, and configuration weaknesses can create persistent pathways through which attackers gain access to operational systems. These results are consistent with previous studies emphasizing that industrial automation and cyber-physical systems remain particularly vulnerable because they often combine long technology life cycles, constrained maintenance windows, heterogeneous architectures, and increasing external connectivity (Akhtar, 2026; Chalyi et al., 2026; Kampourakis et al., 2026; Karras et al., 2025). The positive association between cyber threat exposure and dynamic risk likewise confirms that the frequency and severity of alerts, anomalous activities, unauthorized access attempts, and intrusion indicators materially affect the risk posture of industrial organizations. This supports the broader argument that risk assessment must incorporate not only latent weaknesses but also active threat conditions and changing operational evidence (Paramesha et al., 2024; Pendey, 2023; Vegas & Llamas, 2024).

The negative relationships between dynamic cyber risk and the governance-related variables are equally important. Digital governance capability demonstrated a substantial inverse association with cyber risk, suggesting that stronger oversight, accountability, policy formalization, IT/OT coordination, data stewardship, and managerial control can materially reduce risk even when technical exposure remains present. This supports the proposition that governance is not merely an administrative layer added after technical cybersecurity decisions but an active risk-reduction mechanism. Strong governance can accelerate remediation, clarify responsibility, prioritize critical assets, improve escalation procedures, and reduce organizational fragmentation. These findings align with previous research that treats digital governance as a central determinant of cyber resilience and risk management quality (Ibokette et al., 2024; Liang & WeiweiSun, 2025; Mızrak, 2024; Olabanji et al., 2024). In the context of industrial automation, this is particularly relevant because responsibility for cyber risk is often

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

distributed across engineering, operations, information technology, cybersecurity, management, compliance, and external vendors. Without clear governance mechanisms, even technically mature organizations may experience delayed action or inconsistent control implementation.

Security control effectiveness showed the strongest protective association with dynamic cyber risk among the risk-reducing variables. This finding confirms the practical importance of effective access control, network segmentation, monitoring, configuration management, detection, and response mechanisms in reducing the likelihood that vulnerabilities will translate into successful attacks. Although governance establishes the conditions under which cybersecurity is managed, security controls provide the operational barrier that directly reduces attack success and limits propagation. This distinction is consistent with studies emphasizing the complementary role of strategic governance and technical control systems in contemporary cyber defense (Familoni, 2024; Mohammed, 2024; Onih et al., 2024). The result also reinforces the need to assess control effectiveness dynamically. A control that exists formally but is poorly configured, inconsistently enforced, or inadequately monitored may provide limited risk reduction. Therefore, the quality and actual performance of security controls are more informative than their nominal presence.

Predictive analytics capability also demonstrated a significant negative association with dynamic cyber risk, supporting one of the central assumptions of the present study. Organizations with stronger capabilities in anomaly detection, historical pattern analysis, forecasting, threat intelligence integration, and real-time monitoring reported lower levels of dynamic cyber risk. This result suggests that predictive capability contributes not only to earlier detection but also to improved prioritization and more efficient allocation of security resources. Predictive systems can help identify weak signals before they develop into operationally significant incidents, particularly when risk emerges from multiple interacting indicators rather than a single obvious event. The finding is consistent with studies highlighting the role of artificial intelligence, machine learning, and advanced analytics in strengthening proactive cybersecurity and early-warning capacity (Almotawkel et al., 2026; Lou et al., 2025; Olaore & Alkhwaldi, 2026; Sufi & Alsulami, 2025; Thapaliya & Bokani, 2024). However, the comparatively lower descriptive mean for predictive analytics capability also suggests that this is an area where many organizations have not yet achieved the same maturity as traditional governance or control functions.

The multivariate regression findings provide further insight into the relative importance of the study variables. The integrated model explained approximately 68% of the variance in dynamic cyber risk, which indicates that the combination of technical, governance, and analytical factors provides substantial explanatory power. Industrial automation vulnerability remained the strongest positive predictor, followed by cyber threat exposure. Security control effectiveness emerged as the strongest negative predictor, while digital governance capability, predictive analytics capability, and cybersecurity governance each contributed independently to reducing risk. This finding is especially important because it demonstrates that the protective effect of governance and analytics remains significant even after accounting for technical vulnerability and threat exposure. In other words, organizations facing similar technical risk profiles may experience different overall risk levels depending on their governance maturity, control effectiveness, and ability to interpret and act on predictive information. This is consistent with integrated cybersecurity perspectives that emphasize the interaction between technical exposure and organizational capacity (Chahal, 2023; Harrath et al., 2025; Rananga & Venter, 2026; Rath et al., 2025). The results therefore challenge risk models that rely primarily on vulnerability severity or incident frequency without incorporating organizational response capacity.

The predictive modeling results further demonstrated that machine-learning approaches outperformed conventional logistic regression. Random forest, gradient boosting, and extreme gradient boosting each produced higher accuracy, F1 scores, and AUC values than the baseline model, with extreme gradient boosting achieving the strongest overall performance. The superior performance of the nonlinear ensemble models indicates that dynamic cyber risk is shaped by complex interactions and threshold effects that are not fully captured through conventional linear relationships. This result is consistent with the growing use of ensemble learning and advanced predictive techniques for cybersecurity applications, where heterogeneous inputs and nonlinear dependencies are common (Dayakar Babu Kancherla Prof. Nishant, 2024; Eskandarany, 2024; Gupta, 2024). The strong AUC achieved by the final model suggests that the integrated framework was effective in distinguishing elevated-risk from lower-risk conditions. This finding supports the broader argument that industrial cyber risk assessment can benefit

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

from machine-learning models capable of processing multiple streams of technical and organizational information simultaneously.

The incremental model comparison provides perhaps the strongest evidence for the added value of governance integration. The technical-only model performed reasonably well, but predictive performance improved when security-control variables were added, improved further when digital governance was incorporated, and reached its highest level in the full model that also included predictive analytics capability. The progressive increase in AUC and decrease in the Brier score indicate that governance and analytics improved both discrimination and probability calibration. This finding has direct theoretical implications because it shows that digital governance contributes measurable predictive information beyond what is already contained in vulnerability and threat indicators. Previous studies have increasingly argued that digital transformation, cybersecurity governance, resilience, and analytics should be considered as interdependent dimensions of organizational risk management rather than isolated functions (Antonio João Gonçalves de et al., 2023; Kamuangu, 2025; Liang & WeiweiSun, 2025; Mhlanga, 2026). The present results empirically reinforce that argument by demonstrating that governance variables improve the predictive quality of a cyber risk model rather than merely providing explanatory context after the fact.

The findings also underscore the importance of integrating predictive analytics within an appropriate governance structure. Predictive systems can identify patterns, generate risk probabilities, and prioritize anomalies, but their value depends on whether organizations have the authority structures and decision procedures necessary to respond. Without governance, predictive outputs may remain informational rather than actionable. Conversely, governance without analytical capability may result in well-defined responsibilities but inadequate situational awareness. The study therefore supports a complementary relationship between governance and analytics. This interpretation is consistent with research emphasizing the importance of transparency, accountability, model oversight, and organizational alignment when artificial intelligence and advanced analytics are used in high-stakes decision environments (Andrei & Scarlat, 2024; Islam, 2024; Picano, 2025; Pochmara & Świetlicka, 2024). Within industrial automation, where false negatives may expose critical infrastructure and false positives may disrupt production unnecessarily, the combination of predictive accuracy and governance discipline is particularly important.

The integrated model shown in Figure 1 reflects this combined interpretation. Industrial automation vulnerability and cyber threat exposure act as risk-enhancing drivers, while security control effectiveness, digital governance capability, predictive analytics capability, and cybersecurity governance operate as risk-reducing mechanisms. The model also incorporates continuous operational inputs, including vulnerability severity, asset criticality, incident frequency, real-time monitoring, historical logs, and threat intelligence. This structure is consistent with the increasingly dynamic understanding of cyber risk in contemporary industrial environments (Manowska & Syta, 2026; Picano, 2025; Vegas & Llamas, 2024). Rather than assigning risk at a single point in time, the framework assumes that cyber risk should be continuously recalculated as new technical and organizational evidence becomes available. This is particularly important in industrial systems, where changes in connectivity, threat activity, configuration, and control effectiveness can rapidly alter the practical significance of existing vulnerabilities.

The results also have implications for cyber resilience. Dynamic risk assessment should not be interpreted merely as a prediction mechanism but as part of a broader organizational capacity to anticipate, absorb, respond to, and recover from cyber events. Predictive analytics can provide earlier warning, governance can coordinate decision-making, and effective controls can reduce both attack probability and impact. These elements together support a more resilient security posture. Previous research has similarly emphasized that cybersecurity effectiveness depends on preparedness, coordinated response, and adaptive learning rather than prevention alone (Almotawkel et al., 2026; Familoni, 2024; Mızrak, 2024; Sufi & Alsulami, 2025). The present study extends this perspective by showing that these capabilities can be incorporated into a predictive framework rather than being treated solely as post-incident resilience factors.

Several limitations should be considered when interpreting the findings. First, the study was conducted among professionals and industrial organizations located in Tehran, which may limit the generalizability of the results to other national, regulatory, technological, and industrial contexts. Second, part of the dataset relied on self-reported assessments of governance maturity, control effectiveness, resilience, and predictive capability, which may be influenced by perception bias or organizational desirability. Third, although operational indicators were incorporated into the analysis, the availability and granularity of such data were not necessarily identical across all participating organizations. Fourth, the predictive models were evaluated within

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

the available dataset and therefore require additional external validation before being generalized to different industrial sectors or cybersecurity environments. Fifth, the study focused on organizational and technical predictors but did not comprehensively model human behavioral variables such as employee security behavior, insider threat, operator fatigue, or social engineering susceptibility. Finally, although the framework was designed to be dynamic, the temporal observation window remained limited, and longer-term data could reveal changes in model performance, concept drift, and evolving attack patterns.

Future research should validate the proposed framework across different industries, geographical regions, and regulatory environments and should incorporate larger longitudinal datasets containing higher-frequency operational telemetry. Comparative studies could evaluate whether the relative importance of governance, technical exposure, and predictive capability differs between energy systems, manufacturing, transportation, healthcare infrastructure, and other automation-intensive sectors. Future models should also incorporate human-factor variables, third-party and supply-chain exposure, software dependency risk, and organizational security culture. Additional research could compare extreme gradient boosting with deep learning, temporal neural networks, graph-based models, and hybrid anomaly-detection architectures to determine whether more complex methods improve early-warning performance without sacrificing interpretability. Further work should also examine model drift, recalibration frequency, adversarial manipulation of predictive systems, and the robustness of cyber risk scores under incomplete or noisy data. External validation with real incident outcomes and cross-organizational datasets would be particularly valuable for determining whether the proposed framework can support standardized industrial cyber risk benchmarking.

From a practical perspective, industrial organizations should avoid relying exclusively on static vulnerability scores or periodic compliance assessments and should instead develop continuously updated risk-monitoring processes that integrate technical, operational, and governance information. Organizations should strengthen network segmentation, patch governance, access control, anomaly detection, and industrial asset monitoring while simultaneously clarifying ownership of cyber risk across IT, OT, engineering, management, and compliance functions. Predictive analytics should be incorporated into security operations to support early warning, prioritization, and scenario-based decision-making, but analytical outputs should be governed through clear validation, escalation, and accountability procedures. Organizations should also routinely compare technical exposure with governance maturity and control effectiveness because apparently similar vulnerability profiles may produce very different levels of residual risk. The strongest practical approach is therefore an integrated one in which technical controls, governance, operational monitoring, resilience planning, and predictive analytics function as a coordinated cyber risk management system rather than as isolated organizational activities.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Akhtar, J. (2026). Digital Transformation of Flight Dispatch Operations Through Cloud Based Decision Support Systems. https://doi.org/10.21203/rs.3.rs-10595351/v1

Almotawkel, N. A. A., Alkohali, M. A. S., manaa, s. a. y., Al-Maamari, O. A., Al-Godami, A., & Alqahoom, S. (2026). Zero Trust for IT Governance and Risk Management: A Systematic Review and Conceptual Framework. https://doi.org/10.21203/rs.3.rs-10392666/v1

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Andrei, N., & Scarlat, C. (2024). Marine Applications: The Future of Autonomous Maritime Transportation and Logistics. https://doi.org/10.5772/intechopen.1004275
Antonio João Gonçalves de, A., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*, *12*(8), 1920. https://doi.org/10.3390/electronics12081920
Chahal, S. M. S. (2023). Navigating Financial Evolution: Business Process Optimization and Digital Transformation in the Finance Sector. *International Journal of Finance*, *8*(5), 67-81. https://doi.org/10.47941/ijf.1475
Chalyi, O., Driaunys, K., Grigaliūnas, Š., & Brūzgienė, R. (2026). Standard-Oriented Architecture for AI-Powered Information Security Risk Management. *Electronics*, *15*(6), 1282. https://doi.org/10.3390/electronics15061282

Dayakar Babu Kancherla Prof. Nishant, R. (2024). The Development of New Cyber Security and Networking Solutions Using Artificial Intelligence and Machine Learning. *Journal of Informatics Education and Research*, *3*(2). https://doi.org/10.52783/jier.v3i2.462
Eskandarany, A. (2024). Adoption of Artificial Intelligence and Machine Learning in Banking Systems: A Qualitative Survey of Board of Directors. *Frontiers in Artificial Intelligence*, *7*. https://doi.org/10.3389/frai.2024.1440051
Familoni, B. T. (2024). Cybersecurity Challenges in the Age of Ai: Theoretical Approaches and Practical Solutions. *Computer Science & It Research Journal*, *5*(3), 703-724. https://doi.org/10.51594/csitrj.v5i3.930
Gupta, D. (2024). The Role of Automation in Enhancing Cybersecurity: A Technical Analysis. *International Journal for Multidisciplinary Research*, *6*(5). https://doi.org/10.36948/ijfmr.2024.v06i05.29483
Harrath, Y., Adohinzin, O., Kaabi, J., & Saathoff, M. (2025). Bridging Domains: Advances in Explainable, Automated, and Privacy-Preserving AI for Computer Science and Cybersecurity. *Computers*, *14*(9), 374. https://doi.org/10.3390/computers14090374
Ibokette, A. I., Ogundare, T. O., Anyebe, A. P., Alao, F. O., Odeh, I. I., & Okafor, F. C. (2024). Mitigating Maritime Cybersecurity Risks Using AI-Based Intrusion Detection Systems and Network Automation During Extreme Environmental Conditions. *International Journal of Scientific Research and Modern Technology*, *3*(10), 65-91. https://doi.org/10.38124/ijsrmt.v3i10.73
Islam, M. S. (2024). Guardians of the Web: The Evolution and Future of Website Information Security. https://doi.org/10.20944/preprints202407.0108.v1
Kampourakis, K. E., Gkioulos, V., & Katsikas, S. K. (2026). Cybersecurity Digital Twins for Industrial Systems: From Literature Synthesis to Framework Design. *Information*, *17*(3), 286. https://doi.org/10.3390/info17030286
Kamuangu, P. (2025). Exploring the Convergence of Cybersecurity, Fintech and Artificial General Intelligence: Innovations and Implications. *Abhigyan*, *43*(4), 362-384. https://doi.org/10.1177/09702385251379163
Karras, A., Theodorakopoulos, L., Karras, C., Theodoropoulou, A., Kalliampakou, I., & Kalogeratos, G. (2025). LLMs for Cybersecurity in the Big Data Era: A Comprehensive Review of Applications, Challenges, and Future Directions. *Information*, *16*(11), 957. https://doi.org/10.3390/info16110957
Liang, J., & WeiweiSun. (2025). Integrating Big Data and AI for Network Security in 6G to Enhance University Financial Management. *Internet Technology Letters*, *8*(5). https://doi.org/10.1002/itl2.70106
Lou, H. H., Richmond, P. C., Cai, T., Liu, X., Tsado, L. K., Yoo, J., & Sabuj, M. A. (2025). Integrating Cybersecurity Into Chemical Engineering Education. *International Journal of Information and Communication Technology Education*, *21*(1), 1-20. https://doi.org/10.4018/ijicte.393451
Manowska, A. M., & Syta, J. (2026). Application of Large Language Models in the Protection of Industrial IoT Systems for Critical Infrastructure. *Applied Sciences*, *16*(2), 730. https://doi.org/10.3390/app16020730
Mhlanga, D. (2026). Artificial Intelligence Governance and Sustainable Industrial Transformation in the Era of Industry 5.0. *Sustainability*, *18*(17), 8992. https://doi.org/10.3390/su18178992
Mızrak, F. (2024). Integrating AI With Aviation Cybersecurity: The Strategic Role of Human Resources<sup></Sup&gt. *Business and Management Studies an International Journal*, *12*(3), 610-628. https://doi.org/10.15295/bmij.v12i3.2396
Mohammed, B. (2024). The Impact of Artificial Intelligence on Cyberspace Security and Market Dynamics. *Brazilian Journal of Technology*, *7*(4), e74677. https://doi.org/10.38152/bjtv7n4-019
Olabanji, S. O., Marquis, Y. A., Adigwe, C. S., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*, *17*(3), 57-74. https://doi.org/10.9734/ajrcos/2024/v17i3424
Olaore, O. J., & Alkhwaldi, A. F. (2026). AI-Enhanced Multi-Criteria Decision Support for Cybersecurity Risk Framework Selection: A Machine Learning Comparative Analysis of NIST CSF, ISO 27001, FAIR, OCTAVE and CRAMM. *Journal of Cybersecurity and Privacy*, *6*(4), 127. https://doi.org/10.3390/jcp6040127
Onih, V., Sevidzem, Y. S., & Adeniji, S. (2024). The Role of AI in Enhancing Threat Detection and Response in Cybersecurity Infrastructures. *International Journal of Scientific and Management Research*, *07*(04), 64-96. https://doi.org/10.37502/ijsmr.2024.7404
Paramesha, M., Rane, N., & Rane, J. (2024). Artificial Intelligence, Machine Learning, Deep Learning, and Blockchain in Financial and Banking Services: A Comprehensive Review. https://doi.org/10.2139/ssrn.4855893
Pendey, B. (2023). Artificial Intelligence and Cyber Security. *Journal Transnational Universal Studies*, *1*(2), 93-99. https://doi.org/10.58631/jtus.v1i2.15
Picano, E. (2025). Welcome to the Machine (WTTM): A Cybersecurity Framework for the Automotive Sector. *Electronics*, *14*(18), 3645. https://doi.org/10.3390/electronics14183645
Pochmara, J., & Świetlicka, A. (2024). Cybersecurity of Industrial Systems—A 2023 Report. *Electronics*, *13*(7), 1191. https://doi.org/10.3390/electronics13071191
Rahman, M. M., Pokharel, B. P., Sayeed, S. A., Bhowmik, S., Kshetri, N., & Eashrak, N. (2024). riskAIchain: AI-Driven IT Infrastructure—Blockchain-Backed Approach for Enhanced Risk Management. *Risks*, *12*(12), 206. https://doi.org/10.3390/risks12120206
Rananga, N., & Venter, H. S. (2026). An Anti-Sheriff Cybersecurity Audit Model: From Compliance Checklists to Intelligence-Supported Cyber Risk Auditing. *Applied Sciences*, *16*(5), 2315. https://doi.org/10.3390/app16052315
Rath, S., Pandey, M., & Rautaray, S. S. (2025). Synergistic Review of Automation Impact of Big Data, AI, and ML in Current Data Transformative Era. *F1000research*, *14*, 253. https://doi.org/10.12688/f1000research.161477.2

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Shoetan, P. O., Amoo, O. O., Okafor, E. S., & Olorunfemi, O. L. (2024). Synthesizing Ai's Impact on Cybersecurity in Telecommunications: A Conceptual Framework. *Computer Science & It Research Journal*, *5*(3), 594-605. https://doi.org/10.51594/csitrj.v5i3.908

Sufi, F. K., & Alsulami, M. (2025). Quantifying Temporal Dynamics in Global Cyber Threats: A GPT-Driven Framework for Risk Forecasting and Strategic Intelligence. *Mathematics*, *13*(10), 1670. https://doi.org/10.3390/math13101670

Thapaliya, S., & Bokani, A. (2024). Leveraging Artificial Intelligence for Enhanced Cybersecurity: Insights and Innovations. *Sadgamaya*, *1*(1), 46-52. https://doi.org/10.3126/sadgamaya.v1i1.66888

Vegas, J., & Llamas, C. (2024). Opportunities and Challenges of Artificial Intelligence Applied to Identity and Access Management in Industrial Environments. *Future Internet*, *16*(12), 469. https://doi.org/10.3390/fi16120469

Zulfigarzada, S., Gadirli, A., Karimov, J., Černeckas, D., Račkienė, R., & Ažubalis, M. (2026). Cybersecurity Requirements and Certification Standards in Industrial Automation Systems: A Systematic Review. *Computers*, *15*(6), 364. https://doi.org/10.3390/computers15060364

Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.