Business Risk Analytics for Insider Threat Prevention in Data-Driven Organizations: An Entropy-Based Decision Framework

Liang Chen[1], Yuting Zhao[2], Han Xu[3, *]

[1]School of Management Science and Engineering, Anhui University of Finance and Economics, Bengbu 233030, China

[2]School of Information Management, Shandong Technology and Business University, Yantai 264005, China

[3]School of Business Administration, Henan University of Economics and Law, Zhengzhou 450046, China

*Email: hanxu@huel.edu.cn (Corresponding Author)

Abstract

Insider threat prevention has become a business analytics problem as much as a technical cybersecurity problem. Data-driven organizations depend on privileged employees, cloud platforms, analytics pipelines, and shared data assets, yet conventional insider threat programs often emphasize post-incident detection rather than pre-incident risk measurement. This study develops an entropy-based decision framework for business risk analytics that converts multi-source organizational indicators into interpretable insider risk scores and prevention priorities. The proposed framework integrates human behavior indicators, organizational management conditions, technical safeguard maturity, and data asset exposure into a unified business risk index. Instead of treating insider threat as a binary security event, the framework evaluates the uncertainty embedded in risk indicators and uses entropy weighting to identify which factors contribute most strongly to residual business exposure. A simulated organizational dataset of 640 employee-role observations across five business units is used to demonstrate the framework, including indicator normalization, entropy weight estimation, risk segmentation, mitigation scenario analysis, and managerial decision mapping. Results show that data asset criticality, access-control weakness, abnormal work-pattern signals, and role-pressure indicators generate the largest weighted contributions to insider risk. Scenario analysis further indicates that targeted mitigation focused on the top 25% of high-contribution indicators reduces the overall business risk index by 31.8%, while broad but unfocused controls reduce it by only 12.4%. The study contributes a practical analytics framework that supports early warning, explainability, and resource allocation for insider threat prevention in data-driven organizations.

Keywords: Insider threat prevention; business risk analytics; entropy weighting; data-driven organizations; information security governance; risk decision framework

Article History:

Received: January 16, 2024

Revised: March 18, 2024

Accepted: May 21, 2024

Available Online: June 30, 2024

 https://doi.org/10.63646/jbda.2024.020202

Business Risk Analytics for Insider Threat Prevention in Data-Driven Organizations: An Entropy-Based Decision Framework

1. Introduction

Data-driven organizations create value by collecting, integrating, and analyzing information at a speed and scale that were not possible in traditional business environments. Customer profiles, transaction histories, production records, pricing algorithms, code repositories, digital workspaces, and financial dashboards are increasingly connected through cloud services and internal analytics platforms. This integration improves decision quality, yet it also creates a difficult security management problem: legitimate insiders often have the exact permissions, contextual knowledge, and process access needed to bypass external defenses. As a result, insider threat prevention has moved from the boundary of information security into the core of business risk management.

The business consequences of insider threat events are not limited to technical repair costs. An unauthorized download of customer data may trigger regulatory investigation, contract termination, reputational damage, executive accountability, and loss of market confidence. A privileged employee who manipulates business analytics data can distort management decisions long before a formal breach is detected. A dissatisfied analyst, developer, or operations manager may not begin as a malicious actor, but risk may increase when work pressure, weak supervision, excessive privilege, and sensitive data exposure overlap. For this reason, organizations require a preventive analytics approach that identifies risk-driving conditions before they become incidents.

A large body of insider threat research focuses on detection after abnormal digital behavior has already occurred. Techniques based on anomaly detection, user behavior analytics, network logs, deep learning, and access monitoring are important, but they often face three practical limitations. First, labeled insider threat events are rare and sensitive, making supervised learning difficult. Second, high-risk conditions may exist before suspicious log activity appears. Third, purely technical detection does not adequately explain why a person or business unit has become risky, which weakens managerial response. A business analytics approach should therefore link technical signals with organizational and human factors, while producing interpretable outputs that managers can use to allocate prevention resources.

This study develops an entropy-based decision framework for insider threat prevention in data-driven organizations. The framework is inspired by multi-factor risk measurement research that treats insider threat as a function of human, organizational, and technical drivers. However, the present study reframes the problem as a business risk analytics task. The aim is not to label an employee as malicious, but to evaluate the level of residual business exposure created by uncertain risk indicators, weak controls, sensitive data access, and organizational stressors. This framing is important because firms rarely have perfect evidence of malicious intent. They often have partial, noisy, and unevenly distributed indicators. Entropy weighting is well suited to this context because it assigns greater analytical importance to indicators that contain more discriminating information across the observed population.

The central research question is: how can a data-driven organization convert heterogeneous insider threat indicators into interpretable business risk priorities before an incident occurs? To answer this question, the study proposes a five-stage framework: indicator design, data

 https://doi.org/10.63646/jbda.2024.020202

normalization, entropy weighting, business risk scoring, and decision mapping. The framework is demonstrated using a simulated dataset that represents employee-role observations across analytics, platform operations, finance operations, customer data, and research and development units. The simulation is not intended to represent one real company. Instead, it provides a transparent and reproducible structure for illustrating how the framework works when organizations combine behavioral, organizational, technical, and asset-level indicators.

The contributions of this study are fourfold. First, it extends insider threat analysis from security-event detection to business risk analytics by connecting prevention decisions with measurable exposure drivers. Second, it introduces an entropy-based scoring structure that reduces arbitrary weighting and improves interpretability when indicators differ in dispersion and informational content. Third, it offers a scenario-based evaluation of mitigation strategies, comparing broad control expansion with targeted intervention based on weighted risk contribution. Fourth, it translates analytical results into managerial actions, including access redesign, workflow adjustment, data asset protection, and governance review. These contributions are especially relevant for organizations that have strong data capabilities but lack a practical bridge between cybersecurity monitoring and executive risk management.

The remainder of this article is organized as follows. Section 2 reviews literature on insider threat prevention, business risk analytics, entropy-based assessment, and data-driven governance. Section 3 presents the conceptual framework and indicator taxonomy. Section 4 explains the entropy-based decision method. Section 5 describes the simulated data design and implementation procedure. Section 6 reports empirical-style results and scenario analysis. Section 7 discusses managerial implications and governance recommendations. Section 8 concludes with limitations and future research directions.

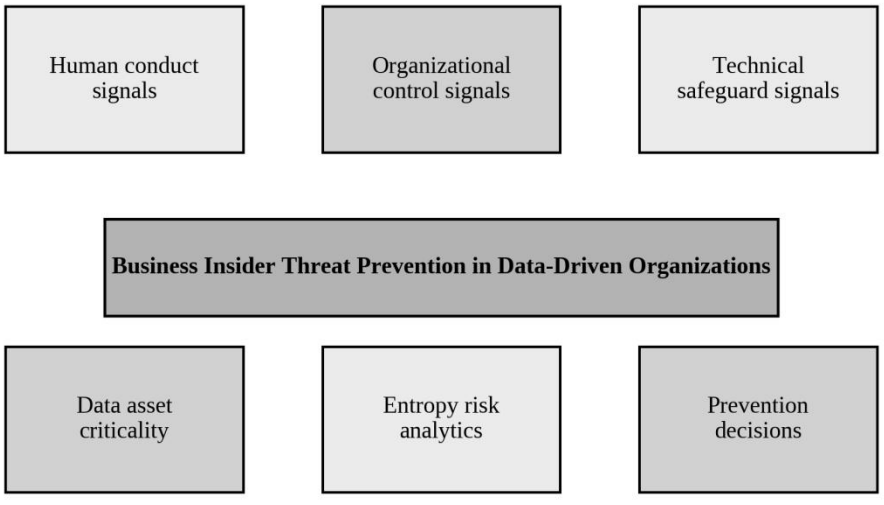


Figure 1. Business risk analytics architecture for insider threat prevention in data-driven organizations.

 https://doi.org/10.63646/jbda.2024.020202

2. Literature Review

2.1 Insider Threat as a Business Risk Problem

Insider threat is best understood as a socio-technical business risk created when legitimate access, sensitive assets, weak controls, and human decision contexts intersect. Information security compliance studies show that employee behavior is shaped by awareness, perceived response efficacy, deterrence beliefs, and organizational norms, rather than by technical rules alone (Bulgurcu et al., 2010). This view supports the present article's decision to model insider exposure as an organizational risk condition rather than as a narrow post-incident security label.

From a business perspective, the damage caused by insider threat is multidimensional. Direct losses may include stolen data, operational interruption, fraud, intellectual property leakage, and recovery expenses. Indirect losses may include customer distrust, regulatory penalties, contract disputes, and management distraction. These consequences affect business continuity and strategic performance, not merely the information technology department. Therefore, insider threat prevention should be located within enterprise risk management and business analytics governance rather than treated as a narrow system-administration issue.

A key weakness of many insider threat programs is their heavy reliance on incident-centric thinking. Organizations often invest in detection rules and forensic capabilities after a breach, but they lack risk measurement tools that show where prevention resources should be deployed before an event occurs. This creates a gap between security operations and executive decision-making. Security teams may see technical alerts, while managers need interpretable evidence about business units, work processes, sensitive assets, and organizational controls. Business risk analytics can fill this gap by converting diverse signals into structured, explainable risk scores that support resource allocation.

2.2 Human, Organizational, and Technical Risk Drivers

Research on insider threat increasingly recognizes the need to integrate human, organizational, and technical indicators. Human-level indicators may include abnormal work patterns, policy violations, job dissatisfaction, sudden changes in behavior, financial pressure, and unusual access behavior. Organizational indicators may include weak supervision, unclear job boundaries, poor communication, excessive workload, unfair rewards, and inadequate training. Technical indicators may include excessive privileges, weak authentication, missing encryption, poor monitoring coverage, and inadequate incident response capability. The value of a multi-factor view is that it avoids the misleading assumption that insider risk is either purely psychological or purely technical.

In data-driven organizations, this multi-factor structure becomes more complex because business units vary in data asset exposure. An analyst in a customer data unit may have access to sensitive information that is far more valuable than the data available to a marketing intern, even if their behavioral signals look similar. A developer with production deployment rights may create greater operational risk than an employee with only read access. Business risk analytics must therefore consider not only the person and the organization, but also the criticality of the data and process context in which access occurs.

The literature also shows that insider threat is characterized by uncertainty. Some indicators are visible but weak, such as minor policy violations. Others are strong but rare, such as confirmed unauthorized data transfer. Some are organizational rather than individual, such as lack of access review. Because of this uncertainty, weighting indicators only by expert judgment may

introduce bias. A method that learns relative importance from the information structure of the data can improve transparency and reduce dependence on subjective preference.

2.3 Entropy Weighting and Risk Analytics

Entropy is a measure of uncertainty and information dispersion. In decision analytics, entropy weighting is commonly used when multiple indicators must be combined but their relative importance is not known in advance. The core intuition is straightforward: an indicator that barely varies across observations provides limited discriminatory information, while an indicator with meaningful dispersion can help separate low-risk from high-risk cases. Entropy weighting therefore assigns lower weight to indicators with limited variation and higher weight to indicators that contribute more information to the evaluation problem.

Entropy-based evaluation is particularly appropriate for insider threat prevention because organizations often observe many weak signals rather than a few decisive labels. For example, the absence of formal access reviews may be common across all business units and therefore less useful for distinguishing risk differences, even though it remains an important governance weakness. By contrast, a signal such as unusual access outside normal work patterns may vary strongly across roles and may carry greater value for segmentation. The entropy approach does not replace managerial judgment, but it provides a data-grounded starting point for determining where attention should be concentrated.

Business risk analytics requires more than a numerical score. It also requires traceability from the final score to the indicators that produce it. Entropy weighting supports this requirement because the final score can be decomposed into dimension-level and indicator-level contributions. Managers can see whether high risk arises from human behavior, organizational pressure, technical weakness, or data asset exposure. This interpretability is essential for prevention because the appropriate response differs by driver. A behavioral anomaly may require supervisory review, while a technical weakness may require access control redesign.

2.4 Expanded Evidence Base for Business-Oriented Insider Risk Analytics

Business intelligence research explains why analytical value depends on the ability to transform heterogeneous data into decision-relevant evidence (Chen et al., 2012). Security compliance research similarly shows that organizational security outcomes depend on how employees interpret obligations, sanctions, and benefits (Bulgurcu et al., 2010). Management analytics research further argues that decision value emerges when analytical models are linked to managerial action rather than treated as isolated technical artifacts (Lu et al., 2024a). Cyber incident cost research shows that risk analytics must account for business loss, regulatory exposure, and operational disruption together (Romanosky, 2016).

The entropy logic used in this article is grounded in information theory, where dispersion indicates the amount of useful information carried by a signal (Shannon, 1948). Big data analytics capability research suggests that performance gains require alignment between analytics resources and business strategy (Akter et al., 2016). Deterrence and protection motivation research indicates that preventive behavior improves when controls are credible, understandable, and linked to perceived risk (Herath and Rao, 2009). Data governance research shows that ownership, standards, and accountability are necessary when multiple organizational units rely on shared data assets (Khatri and Brown, 2010).

Analytics capability studies emphasize that technology, data, skills, and managerial resources must operate together before data can improve organizational performance (Gupta and George, 2016). Neutralization theory explains why employees may rationalize security violations when rules seem inconvenient, unfair, or weakly enforced (Siponen and Vance, 2010). Recent internal auditing research shows that blockchain-enabled audit trails can strengthen accountability where

traditional controls depend on delayed review (Wu et al., 2025). Economic models of security investment demonstrate that prevention spending should be evaluated against expected loss reduction rather than against technical maturity alone (Gordon and Loeb, 2002).

Information systems research on big data argues that analytical infrastructures reshape how organizations sense, explain, and act on risk (Abbasi et al., 2016). Fear-appeal research shows that security messages affect behavior only when users believe they can perform the recommended protective action (Johnston and Warkentin, 2010). IoT cybersecurity research highlights that connected devices and distributed data flows expand the attack surface that organizations must govern (Lu and Xu, 2019). Cybersecurity situational awareness research supports the need for continuous, multi-source visibility rather than isolated incident reports (Husak et al., 2019).

Empirical studies of analytics capability show that big data produces value when firms combine analytical technologies with dynamic organizational capabilities (Wamba et al., 2017). Security education research indicates that training works best when it changes daily routines rather than merely distributing policy documents (Puhakainen and Siponen, 2010). FinTech research demonstrates that digital platforms expose organizations to combined technological, financial, and governance risks (Kou and Lu, 2025). Machine learning surveys in cybersecurity show that anomaly detection is valuable but still depends on high-quality contextual data and careful interpretation (Buczak and Guven, 2016).

Best-worst method research illustrates how structured weighting can support management decisions when criteria compete for attention (Rezaei, 2015). Big data value research stresses that managers need a clear route from data assets to strategic benefit (Grover et al., 2018).

Information security motivation research shows that compliance behavior is influenced by response costs, self-efficacy, and perceived organizational expectations (Vance et al., 2012). Fuzzy TOPSIS research further shows that subjective and objective weights can be combined when risk indicators are imprecise (Wang and Lee, 2009). Energy-oriented MCDM research also demonstrates that decision frameworks must remain interpretable when many criteria compete for managerial attention (Wang et al., 2009). Blockchain studies in Industry 4.0 show that tamper-resistant records can support traceability in complex digital operations (Chen et al., 2024).

Cybersecurity data science research frames security as a data-intensive analytical domain that requires feature engineering, monitoring, and model interpretation (Sarker et al., 2020). Extensions of the best-worst method show that decision weights should be examined for consistency and practical usability (Rezaei, 2016). Econometric evidence on analytics and firm performance confirms that analytics investments produce different returns across industries and organizational settings (Muller et al., 2018). Misuse research shows that awareness of countermeasures can reduce opportunistic behavior when employees expect violations to be detectable (D'Arcy et al., 2009).

Industry 4.0 research shows that cyber-physical and data-intensive systems make technical, organizational, and human risks more tightly coupled (Lu, 2025). Anomaly detection research provides general methods for identifying unusual observations, but it also warns that anomalies require domain interpretation before managerial action is justified (Chandola et al., 2009). Fuzzy set theory remains useful when organizational risk cannot be expressed as a purely crisp category (Zadeh, 1965). Big data value reviews argue that organizations realize value through interpretation and organizational change, not through data accumulation alone (Gunther et al., 2017).

Security-related stress research shows that demanding controls can create coping responses that increase policy violations when employees perceive requirements as excessive (D'Arcy et al., 2014). Motivation research indicates that employees may follow security policies out of both fear of sanctions and desire for organizational protection (Son, 2011). Artificial intelligence research in industrial information systems shows that AI-enabled decision support should be evaluated

through both technical accuracy and organizational adoption (Zhang and Lu, 2021). Network anomaly detection research shows that abnormal traffic patterns can indicate risk, but false positives require contextual filtering (Ahmed et al., 2016). Fuzzy decision theory indicates that managerial choices under uncertainty can be represented without pretending that every criterion is fully precise (Bellman and Zadeh, 1970).

Research on big data decision-making quality shows that decision value depends on data quality, analytical competence, and process transparency (Janssen et al., 2017). Enterprise policy compliance research suggests that managerial support and perceived fairness influence whether employees treat information security as legitimate (Hu et al., 2012). Artificial intelligence research emphasizes that intelligent analytics should augment human judgment rather than replace accountability in complex decisions (Lu, 2019). Intrusion detection research shows that machine learning models trained in closed environments may perform poorly when operational behavior changes (Sommer and Paxson, 2010).

Priority-scaling research in decision analysis offers a foundation for comparing heterogeneous risk factors in a structured way (Saaty, 1977). Security policy design research indicates that sanctions and rewards should be balanced because purely punitive systems may reduce trust (Chen et al., 2012). Industry 4.0 research shows that connected manufacturing and digital operations require integrated governance of data, automation, and human roles (Lu, 2017). Enterprise data breach research shows that prevention must cover causes, organizational challenges, and future control directions together (Cheng et al., 2017). Cloud security research demonstrates that outsourced and virtualized infrastructures require controls that travel across organizational boundaries (Fernandes et al., 2014).

Fuzzy multi-attribute decision research supports the use of structured scoring when risk drivers differ in measurement scale and uncertainty (Triantaphyllou and Lin, 1996). Unified compliance models show that security behavior draws from multiple behavioral theories, so a single-attitude explanation is incomplete (Moody et al., 2018). Blockchain-IoT security research shows that distributed devices require secure identity, trusted records, and accountable data exchange (Xu et al., 2021). Cloud computing security research stresses that availability, confidentiality, and integrity risks must be considered together when data are stored off-premises (Zissis and Lekkas, 2012).

Entropy-based cross-efficiency research demonstrates how information entropy can reduce arbitrary weight selection in multi-indicator evaluation (Wu et al., 2011). Studies that integrate planned behavior and protection motivation show that employees' compliance intentions depend on perceived risk and perceived ability to comply (Ifinedo, 2012). Cybersecurity culture research argues that secure behavior improves when security becomes a routine organizational practice rather than a periodic campaign (Alshaikh, 2020). Decision-making research in management analytics emphasizes that analytics is most useful when results are understandable to the people who must act on them (Lu et al., 2024b).

Zero trust architecture research supports the idea that access should be continuously verified rather than permanently trusted after login (Rose et al., 2020). Compromise-ranking research in multi-criteria decision making shows how competing criteria can be converted into an actionable priority order (Opricovic and Tzeng, 2004). Behavioral information security reviews call for research that connects technical safeguards with individual and organizational behavior (Crossler et al., 2013). Studies of security-related behavior show that user actions are shaped by cognition, organizational expectations, and the perceived usability of controls (Guo, 2013).

Blockchain implementation research in information systems suggests that trusted infrastructure can support accountability, auditability, and inter-organizational verification (Lu, 2022). Conceptual cybersecurity research shows that the field combines technologies, processes, people, and organizations rather than only network defense (Craigen et al., 2014). Reviews of multi-criteria decision-making applications show that decision methods are most persuasive when

criteria and weights are transparent to stakeholders (Mardani et al., 2015). Information security culture research demonstrates that monitoring and implementation actions can improve security culture when they are combined with feedback and management support (Da Veiga and Martins, 2015).

Cross-national cybersecurity awareness research shows that knowledge, awareness, and behavior are related but not identical, which supports separate measurement of control maturity and human conduct (Zwilling et al., 2022). Cyber risk analytics research argues that AI-enabled industrial and IoT systems require adaptive risk models that can handle changing operational contexts (Radanliev et al., 2020). Prospect theory suggests that managers may overweight salient losses and underweight diffuse prevention benefits, which makes quantified risk reduction important for investment decisions (Kahneman and Tversky, 1979). Knowledge mechanism research shows that security knowledge breadth and depth shape how employees construe threats (Mady et al., 2023).

Blockchain cybersecurity research indicates that distributed ledgers can strengthen privacy and security when governance, scalability, and access-control design are addressed together (Kshetri, 2017). Human-aspects security measurement research provides validated survey constructs that can complement behavioral and access-log indicators (Parsons et al., 2014). Reviews of blockchain applications show that distributed records can support traceability, but value depends on the fit between the application context and the governance mechanism (Casino et al., 2019). Supply chain blockchain research demonstrates that transparency technologies are useful when they solve coordination and trust problems rather than when they are adopted for novelty alone (Saberi et al., 2019).

Database security research emphasizes that confidentiality, integrity, authorization, and auditing are inseparable in data-intensive environments (Bertino and Sandhu, 2005). Role-based access control research provides a practical foundation for aligning permissions with organizational roles and responsibilities (Sandhu et al., 1996). Attribute-based access control research extends this logic by allowing policy decisions to consider attributes of subjects, resources, actions, and context (Hu et al., 2015). Context-aware access control research shows that dynamic environments require policies that adapt to location, time, device, task, and risk conditions (Kayes et al., 2020). Entropy-based fuzzy decision research shows how correlation and uncertainty can be integrated into multi-criteria assessment (Ye, 2010).

Recent insider threat model enhancement research shows that combining supervised learning with outlier scores can improve detection when labeled malicious cases are scarce (Yi et al., 2024). Natural language and sentiment-based insider risk research demonstrates that textual signals can reveal organizational stress, but it also requires privacy safeguards and careful validation before use (Mladenovic et al., 2024). A 2025 systematic review of user-behavior-based insider threat detection further shows that behavioral analytics is useful only when feature selection, validation, and organizational context are considered together (Kamatchi and Uma, 2025). Together, these studies justify the present article's emphasis on interpretable scoring, proportional governance, and targeted prevention rather than automated punishment.

2.5 Research Gap

Existing insider threat studies provide valuable detection models, behavioral frameworks, and security taxonomies. However, three gaps remain. First, many models emphasize event detection rather than pre-incident business risk measurement. Second, technical and human indicators are often analyzed separately, reducing the ability to explain risk as a socio-technical business condition. Third, many scoring approaches rely on fixed expert weights, which may not reflect the information structure of actual organizational data. These gaps limit the usefulness of insider threat analytics for executives who must decide where to invest prevention resources.

This study addresses these gaps by proposing a decision framework that combines multi-factor indicator design with entropy weighting and scenario-based mitigation analysis. The framework is designed for organizations that want to use internal data responsibly, without turning risk scoring into automatic disciplinary action. Its purpose is to prioritize governance attention, identify control weaknesses, and support targeted prevention. The framework therefore treats insider threat analytics as an organizational learning tool rather than a surveillance instrument.

3. Conceptual Framework and Indicator Taxonomy

The proposed framework is built on the premise that insider risk in data-driven organizations emerges from the interaction of four dimensions: human conduct signals, organizational control conditions, technical safeguard maturity, and data asset exposure. Human conduct signals capture observable behavior or role-related conditions that may indicate increased uncertainty. Organizational control conditions capture whether management practices reduce or amplify risk. Technical safeguard maturity captures the strength of authentication, authorization, monitoring, encryption, and incident response. Data asset exposure captures the sensitivity and business criticality of the assets accessible to the role or employee.

The framework does not assume that any single indicator proves malicious intent. Instead, it interprets indicators as risk-relevant observations that may increase or decrease uncertainty. This distinction is important ethically and analytically. A high workload score does not imply misconduct. It may simply indicate that business pressure could raise error probability, resentment, or control bypass behavior. A high asset exposure score does not imply wrongdoing. It indicates that the consequences of misuse would be serious if other risk conditions are also present. The decision framework therefore combines probability-related signals and impact-related signals in a transparent manner.

Table 1. Indicator Taxonomy for Insider Threat Business Risk Analytics

Dimension	Indicator group	Example indicators	Business interpretation
Human conduct signals	Work-pattern and policy behavior	After-hours access, repeated minor policy exceptions, abnormal data query volume, unusual job-role activity	Shows whether the observed role behavior deviates from expected business routines.
Organizational control conditions	Management and process environment	Workload pressure, unclear responsibility, poor communication, weak training, insufficient review of privileged actions	Shows whether the organization creates conditions that amplify or reduce insider risk.
Technical safeguard maturity	Security control effectiveness	Multi-factor authentication, least-privilege enforcement, encryption, monitoring coverage, incident response readiness	Shows whether the technical environment restricts misuse and improves detectability.
Data asset exposure	Sensitivity and process criticality	Customer data access, financial data access, source-code access, model pipeline access, transaction approval rights	Shows potential business impact if a trusted role is misused.
Decision response	Preventive management action	Access redesign, targeted review, training, workflow redesign, automated alert refinement, risk acceptance	Links analytical findings to feasible managerial interventions.

Table 1 organizes the indicator design into business-relevant categories rather than purely technical data fields. This structure enables managers to understand why a business unit or role receives a higher risk score. For example, customer data operations may not show the highest number of behavioral anomalies, yet it may still appear as a high-risk unit because the data asset exposure dimension is elevated. Conversely, an operations unit may show strong behavioral

anomalies but lower business impact if data access is restricted. The framework is therefore flexible enough to distinguish between likelihood-oriented and impact-oriented risk factors.

The indicator taxonomy also supports modular implementation. A small organization may begin with twelve indicators drawn from access logs, human resource records, and control self-assessments. A larger organization may extend the taxonomy with additional indicators such as code repository access, data export frequency, sensitive model interaction, privileged cloud console activity, or separation-of-duties violations. Entropy weighting can be applied at either the full indicator level or a higher dimension level, depending on data availability and governance maturity.

4. Entropy-Based Decision Framework

4.1 Analytical Logic

The proposed decision framework converts multi-source indicator data into a business insider risk index through five steps. The first step defines the indicator set and assigns each indicator to a dimension. The second step normalizes indicator values so that higher values consistently represent higher risk. The third step estimates entropy weights based on the dispersion of each indicator across observations. The fourth step calculates dimension-level and overall risk scores. The fifth step maps the results into prevention decisions. Figure 2 summarizes the implementation workflow.

The framework requires careful data governance. Indicators should be collected only for legitimate security and risk management purposes. Personally sensitive variables should be minimized, pseudonymized, and reviewed by appropriate governance committees. The framework should not be used as an automated employee punishment mechanism. Its proper use is to identify conditions requiring further review, control improvement, or supportive intervention. This principle is especially important because insider risk is probabilistic and contextual rather than definitive.

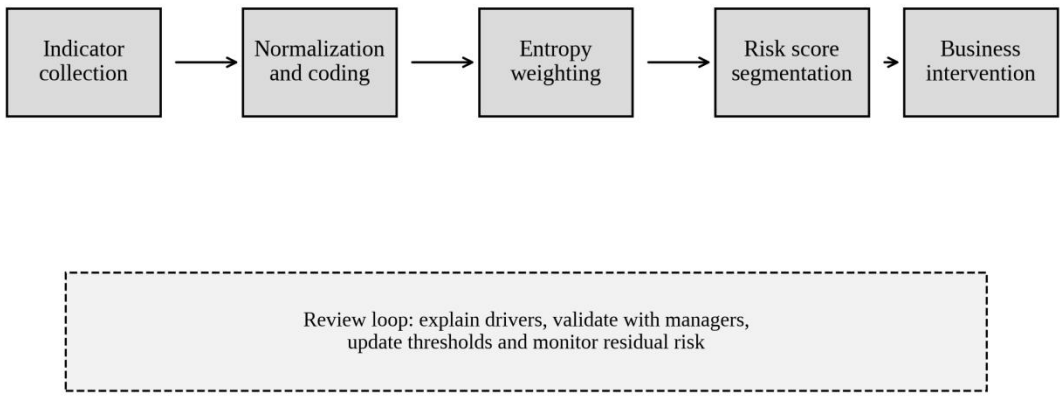


Figure 2. Entropy-based decision workflow for insider threat business risk analytics.

 https://doi.org/10.63646/jbda.2024.020202

4.2 Indicator Normalization and Entropy Weighting

Because insider risk indicators are measured on different scales, normalization is required before aggregation. Binary indicators such as the presence of multi-factor authentication can be coded as 0 or 1 after reversing the scale when necessary. Ordinal indicators such as workload pressure can be transformed to a 0 to 1 interval. Continuous indicators such as abnormal query volume can be winsorized and normalized to reduce distortion from extreme values. The guiding rule is that a larger normalized value should represent greater business risk exposure.

After normalization, entropy weighting evaluates the informational contribution of each indicator. Let xij denote the normalized value of indicator j for observation i. The proportional contribution of observation i to indicator j is calculated and then used to estimate the entropy value of that indicator. Indicators with high dispersion have lower entropy and receive higher weights. Indicators with little variation have higher entropy and receive lower weights. For clarity, the study uses only three compact equations.

$$p_{ij} = x_{ij} / \Sigma_i x_{ij} \quad (1)$$

$$e_j = -k \Sigma_i p_{ij} \ln(p_{ij}) \quad (2)$$

$$BRI_i = \Sigma_j w_j x_{ij} \quad (3)$$

In these expressions, p_{ij} is the normalized proportion of observation i for indicator j, e_j is the entropy value of indicator j, w_j is the entropy-derived weight, and BRIi is the business risk index of observation i. The constant k normalizes entropy to a comparable interval. The equations are intentionally simple because the purpose of the framework is operational decision support rather than mathematical complexity. The method is easy to implement in spreadsheet software, statistical packages, or enterprise analytics platforms.

A major advantage of this weighting logic is that it can be explained to non-technical managers. If an indicator is nearly the same for every role, it cannot effectively separate high-risk from low-risk observations and therefore receives less weight. If an indicator varies substantially and aligns with meaningful differences across business units, it receives more weight. This explanation is more transparent than black-box scoring and less subjective than assigning all weights by expert opinion alone.

4.3 Business Decision Rules

The final risk score should be translated into decision rules that reflect the organization's risk appetite. In this study, risk scores are segmented into four levels. Low risk indicates ordinary monitoring and standard control maintenance. Moderate risk indicates periodic review and targeted training. High risk indicates managerial review, access recertification, and process control assessment. Critical risk indicates immediate risk review, temporary privilege reduction where justified, and investigation of control failure. These levels should not be interpreted as disciplinary labels; they are governance triggers.

Decision rules should combine the overall score with the dominant risk driver. A high score driven by technical weakness requires a different intervention from a high score driven by organizational pressure. If the technical dimension dominates, managers may strengthen authentication, monitoring, and least-privilege controls. If organizational control dominates, managers may revise workload allocation, improve communication, or clarify job responsibilities. If asset exposure dominates, managers may redesign data access, segment sensitive datasets, or require additional approval for exports. This driver-based logic transforms risk scoring into actionable governance.

 https://doi.org/10.63646/jbda.2024.020202

5. Data Design and Analytical Procedure

5.1 Simulated Organizational Dataset

To demonstrate the framework without exposing real employee information, this study uses a simulated organizational dataset. The dataset contains 640 employee-role observations across five business units: analytics, platform operations, finance operations, customer data, and research and development. The simulation represents a medium-sized data-driven enterprise with cloud-based data infrastructure and role-based access management. Each observation includes 28 normalized indicators distributed across the four risk dimensions. The data were generated to reflect plausible organizational patterns, including higher asset exposure in customer data and research and development units, higher workload pressure in platform operations, and stronger technical safeguards in finance operations.

The simulated design has two purposes. First, it illustrates how an organization could implement the method using structured data from access-control systems, human resource records, security training records, data catalog metadata, and control self-assessment tools. Second, it allows transparent scenario analysis. Because no real employees are represented, the results can be discussed openly and reproduced. The framework is designed to be applied to real data only after privacy review, governance approval, and clear internal communication about its purpose.

Table 2. Simulated Data Design and Descriptive Profile

Item	Analytics	Platform Ops	Finance Ops	Customer Data	R&D
Employee-role observations	128	142	116	132	122
Average privileged-access ratio	0.31	0.38	0.29	0.44	0.41
Average workload pressure index	0.42	0.61	0.49	0.55	0.46
Average technical-control gap	0.30	0.47	0.38	0.57	0.52
Average data asset exposure	0.45	0.61	0.67	0.74	0.70
Prior minor policy exceptions per 100 roles	7.8	12.4	8.1	14.6	10.3

Table 2 shows that the simulated business units differ in ways that are meaningful for insider risk analytics. Customer data has the highest data asset exposure and the largest number of prior minor policy exceptions. Platform operations has the highest workload pressure, reflecting continuous service responsibility and urgent operational tasks. Finance operations has high asset exposure but a lower technical-control gap, representing stronger formal control maturity. These differences allow the entropy model to identify not only which units have higher overall scores, but also why those scores emerge.

The analytical procedure followed five steps. First, all indicators were checked for directionality so that larger values represented higher risk. Second, binary indicators were transformed to 0 or 1, and ordinal indicators were rescaled to the 0 to 1 interval. Third, entropy weights were estimated for the 28 indicators and then aggregated to the four dimension levels. Fourth, business risk scores were calculated for each observation and averaged by business unit. Fifth, three mitigation scenarios were simulated: broad control expansion, targeted intervention on high-contribution indicators, and integrated prevention combining access redesign with organizational workflow changes.

5.2 Measurement Validity and Governance Controls

A risk analytics framework is only useful if the measurement process is credible. Four controls are therefore built into the procedure. First, indicators must have business definitions that can be

reviewed by managers and security professionals. Second, each indicator must have a documented data source, update frequency, and owner. Third, high-risk results must be explainable through dimension-level decomposition. Fourth, any action affecting employees must require human review and proportional response. These controls reduce the risk that analytics becomes opaque surveillance.

The use of simulated data in this study also clarifies the boundary between methodological demonstration and empirical claim. The numerical results should be interpreted as analytical evidence about the behavior of the framework under plausible conditions, not as a measured estimate of insider threat prevalence in a real firm. The value of the demonstration lies in showing how entropy weighting changes prioritization and how scenario analysis can compare different prevention strategies.

6. Results and Analysis

6.1 Entropy Weights and Risk Contribution

The entropy weighting procedure produced dimension weights that reflect the informational dispersion of the simulated indicators. Data asset exposure received the highest dimension weight because access to sensitive data and critical processes varied considerably across business units. Technical safeguard maturity received the second-highest weight, driven by variation in monitoring coverage, least-privilege enforcement, and privileged access review. Human conduct signals and organizational control conditions also contributed materially, but their dispersion was slightly lower in the simulated dataset. Table 3 reports the dimension weights and selected indicator contributions.

Table 3. Entropy Weights and Major Risk Contribution Indicators

Dimension	Dimension weight	High-contribution indicator	Indicator weight	Interpretation
Human conduct signals	0.218	Abnormal access timing	0.047	Varies strongly across operations and customer data roles.
Human conduct signals	0.218	Repeated minor policy exceptions	0.039	Captures early behavioral deviation without assuming intent.
Organizational controls	0.203	Workload pressure	0.041	High dispersion between platform operations and analytics roles.
Organizational controls	0.203	Access review delay	0.036	Shows governance lag in role recertification.
Technical safeguards	0.257	Least-privilege gap	0.055	Strongly separates units with broad standing privileges.
Technical safeguards	0.257	Monitoring coverage gap	0.049	Indicates weak visibility over sensitive activity.
Data asset exposure	0.322	Sensitive customer data access	0.063	Raises business impact in customer data operations.
Data asset exposure	0.322	Model pipeline or source-code access	0.052	Raises exposure in R&D and analytics roles.

The results support the central argument of this study: insider threat prevention in data-driven organizations cannot be reduced to behavioral monitoring alone. Data asset exposure is the largest weighted dimension because the potential business impact of misuse depends heavily on what an insider can access. Technical safeguards are also highly weighted because weak least-privilege enforcement and limited monitoring create opportunity. Human conduct signals remain important, but their interpretation is strengthened when they are combined with organizational and technical context.

The indicator-level results are useful for prevention because they show where interventions will likely produce the largest reduction in business exposure. For example, reducing standing

 https://doi.org/10.63646/jbda.2024.020202

privileges in customer data operations would lower both technical-control risk and data asset exposure. Improving workload design in platform operations would reduce organizational pressure but would not fully address asset criticality. This distinction matters because managers often prefer broad training programs, yet the entropy results suggest that some technical and asset-governance controls may yield stronger risk reduction.

6.2 Business Unit Risk Scores

The entropy-weighted scores were aggregated at the business unit level to support managerial interpretation. Figure 3 shows the distribution of human, organizational, technical, asset, and overall risk scores. Customer data has the highest overall risk score, followed by platform operations, finance operations, research and development, and analytics. The ordering is not determined by one factor alone. Customer data scores high because asset exposure and technical-control gaps reinforce one another. Platform operations scores high because workload pressure and access timing anomalies are elevated. Finance operations has high asset exposure, but stronger technical safeguards moderate the overall score.

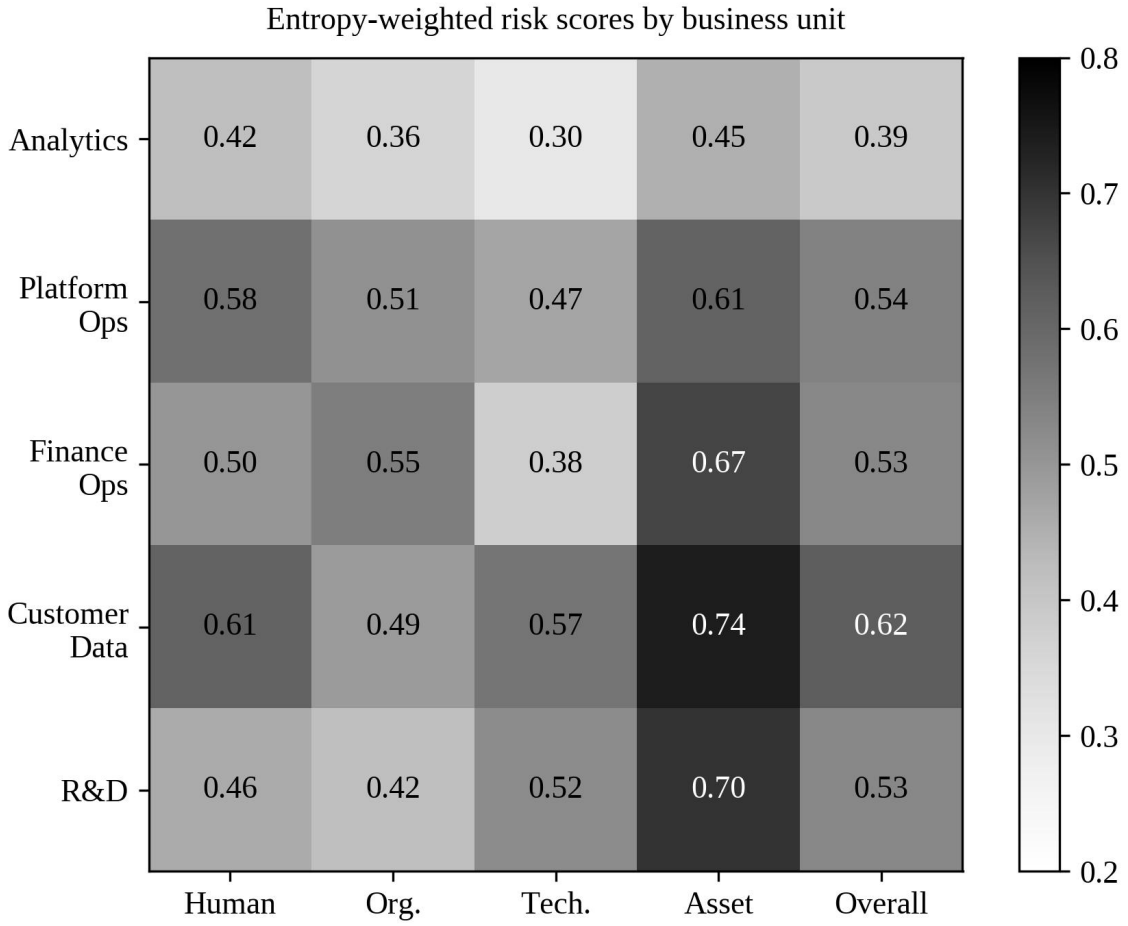


Figure 3. Entropy-weighted risk scores by business unit and dimension.

The heatmap demonstrates the value of dimension-level decomposition. A single overall score would identify customer data as the highest-risk unit, but it would not reveal whether the problem is employee conduct, access design, or asset concentration. The decomposition shows that customer data requires controls focused on sensitive data access and monitoring coverage, while

platform operations requires workload and work-pattern review. This distinction improves the relevance of managerial responses and reduces the likelihood of applying the same intervention to every business unit.

A role-level inspection also showed that 18.6% of observations fell into the high or critical risk segments. Among these observations, 43% were concentrated in customer data, 27% in platform operations, 14% in research and development, 9% in finance operations, and 7% in analytics. This distribution suggests that prevention resources should not be allocated evenly across units. A uniform allocation would overinvest in lower-exposure units and underinvest in high-exposure areas.

Table 4. Business Unit Risk Score Summary and Segment Distribution

Business unit	Mean BRI	Low (%)	Moderate (%)	High (%)	Critical (%)	Dominant driver
Analytics	0.39	42.2	45.3	10.2	2.3	Data access concentration
Platform operations	0.54	21.1	46.5	25.4	7.0	Workload pressure and access timing
Finance operations	0.53	24.1	50.0	20.7	5.2	Asset exposure with moderate controls
Customer data	0.62	13.6	41.7	31.8	12.9	Sensitive customer data and control gaps
Research and development	0.53	25.4	47.5	22.1	5.0	Source-code and model pipeline exposure

Table 4 provides a practical summary for executives. The mean BRI identifies overall exposure, while the segment distribution reveals whether risk is concentrated in a small number of critical observations or spread across a broad population. Customer data has both the highest mean score and the highest critical segment. Platform operations has a lower critical share but a substantial high-risk segment, indicating a need for process-level improvement. Finance operations and research and development have similar mean scores but different dominant drivers, which again confirms the need for differentiated interventions.

The results also show why insider threat prevention should be framed as a business analytics problem. The highest risk does not simply appear where technical alerts are most frequent. It appears where sensitive assets, access privileges, organizational pressure, and control weaknesses intersect. This intersection is exactly what decision-makers need to see when deciding whether to redesign access, add monitoring, change workflow, or accept residual risk.

6.3 Scenario-Based Mitigation Analysis

Three mitigation strategies were evaluated to examine how different management choices affect the business risk index. Scenario A represents broad control expansion, including general training and organization-wide policy reminders. Scenario B represents targeted intervention on the top 25% of high-contribution indicators, including least-privilege redesign, monitoring coverage improvement, and focused review of sensitive data access. Scenario C represents integrated prevention, combining targeted technical controls with workload adjustment and managerial review in the highest-risk units. Each scenario was simulated by reducing relevant normalized indicator values and recalculating entropy-weighted risk scores.

Table 5. Mitigation Scenario Results

Scenario	Primary action	Overall BRI before	Overall BRI after	Risk reduction	Implementation burden
Baseline	No additional mitigation	0.524	0.524	0.0%	None
Scenario A	Broad training and policy reminders	0.524	0.459	12.4%	Low
Scenario B	Targeted intervention on top contribution indicators	0.524	0.357	31.8%	Moderate

 https://doi.org/10.63646/jbda.2024.020202

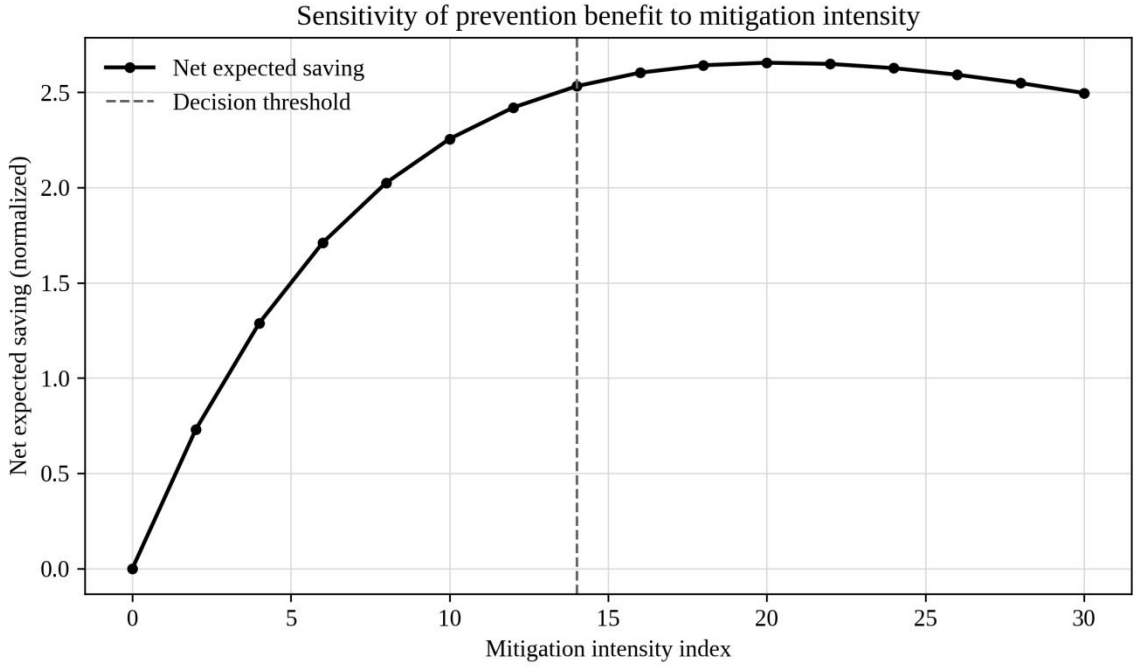
Scenario C	Integrated technical and organizational prevention	0.524	0.331	36.8%	Moderate to high

The scenario results reveal that targeted mitigation is substantially more effective than broad but unfocused action. Scenario A reduces the overall BRI by 12.4%, which is valuable but limited because general training does not directly change asset exposure or least-privilege gaps. Scenario B reduces the BRI by 31.8% by addressing the indicators with the largest weighted contributions. Scenario C produces the largest reduction at 36.8%, but it requires more coordination because it combines technical access redesign with changes in workload and managerial review. The additional improvement of Scenario C over Scenario B is meaningful but smaller than the improvement of Scenario B over Scenario A, indicating that targeted technical and asset controls are the strongest first step.

These findings provide a practical decision rule. Organizations with limited resources should first identify and mitigate high-contribution indicators rather than apply equal effort across all indicators. Once the largest technical and asset-exposure drivers are reduced, organizational interventions can address residual risk that arises from workload pressure, communication gaps, or unclear responsibilities. This staged approach aligns prevention investment with measurable risk contribution.

6.4 Sensitivity Analysis

Sensitivity analysis was conducted to evaluate the relationship between mitigation intensity and expected prevention benefit. Figure 4 shows a stylized net expected saving curve. The curve initially rises because early investments address high-impact weaknesses such as excessive privileges, weak monitoring, and sensitive data export controls. After a threshold, the curve flattens and then declines because additional mitigation becomes more expensive and yields smaller marginal reductions. This pattern is consistent with the economic logic of cybersecurity investment: the first controls usually remove the most obvious and costly risks, while later controls address narrower residual exposures.



 https://doi.org/10.63646/jbda.2024.020202

Figure 4. Sensitivity of prevention benefit to mitigation intensity.

The sensitivity result has two managerial implications. First, underinvestment is risky because the organization leaves high-impact and relatively inexpensive prevention opportunities unused. Second, overinvestment is also inefficient because excessive controls can increase operating friction without proportionate risk reduction. The optimal region lies near the point where marginal risk reduction and marginal implementation burden are balanced. In the simulated case, this region corresponds to targeted controls rather than universal restrictions. Managers should therefore use risk contribution evidence to calibrate control strength by role and asset criticality.

The analysis also suggests that risk scoring should be updated periodically. As controls improve, the entropy structure of indicators may change. An indicator that once separated high-risk from low-risk roles may become less informative after remediation. Conversely, a new indicator may become more important as business processes change. Periodic recalculation helps the risk analytics system remain adaptive rather than locked into outdated assumptions.

7. Discussion and Managerial Implications

7.1 From Detection to Prevention

The results support a shift from incident detection to preventive risk analytics. Detection remains necessary, but it is not sufficient for data-driven organizations where insiders may create harm before conventional alerts are triggered. The proposed framework enables managers to identify risk-concentrated roles, business units, and control weaknesses before an incident occurs. This does not mean predicting individual misconduct with certainty. Rather, it means recognizing conditions under which insider misuse would be more likely, more damaging, or harder to detect.

A prevention-oriented approach is especially important because many insider incidents are preceded by ordinary organizational signals rather than dramatic technical anomalies. Workload pressure, privilege creep, weak review routines, unclear job boundaries, and sensitive data concentration may be visible long before an incident. By integrating these signals, managers can intervene through process redesign, access recertification, supportive supervision, and targeted monitoring. This approach is more balanced and defensible than relying only on aggressive surveillance after technical alerts appear.

7.2 Designing Responsible Insider Risk Analytics

Responsible implementation requires clear governance. First, the purpose of insider risk analytics should be documented as risk prevention and control improvement, not employee profiling. Second, the indicator set should exclude unnecessary sensitive personal attributes. Third, high-risk classifications should require human review and contextual interpretation. Fourth, employees should be informed that access to sensitive data is governed by risk-based controls. Fifth, the organization should audit the model for bias, data quality problems, and unintended consequences. These governance measures protect both the organization and employees.

Model explainability is central to legitimacy. A manager should be able to understand why a role or unit appears as high risk. If the score is driven by technical safeguards, the response should address technical controls. If it is driven by organizational stress, the response should address work design. If it is driven by asset exposure, the response should address data segmentation and access approval. The entropy framework supports this explainability because it decomposes overall risk into weighted indicator contributions.

 https://doi.org/10.63646/jbda.2024.020202

7.3 Resource Allocation and Control Prioritization

The scenario analysis demonstrates that targeted intervention provides stronger risk reduction than broad action. This finding matters for executives because prevention budgets are limited. Many organizations respond to insider risk by increasing general training or issuing policy reminders. Such actions are useful, but they rarely change the structural drivers of risk. The framework shows that reducing least-privilege gaps, improving monitoring coverage, and protecting sensitive data assets may provide larger risk reductions than broad education alone. Training should support these controls, not substitute for them.

A practical resource allocation strategy can follow three steps. First, identify the top-contribution indicators at the enterprise level. Second, identify the business units where those indicators are most concentrated. Third, select interventions that directly reduce the relevant indicator values. For example, if sensitive customer data access is the dominant driver in customer data operations, the intervention may include data masking, approval workflow, export limitation, and quarterly access review. If abnormal access timing is dominant in platform operations, the response may include shift-based access rules, exception logging, and review of emergency access procedures.

Table 6. Decision Mapping from Risk Drivers to Prevention Actions

Dominant risk driver	Analytical signal	Recommended prevention action	Expected business effect
Excessive asset exposure	High data asset score and broad privileges	Segment sensitive data, apply least privilege, require additional approval for exports	Reduces impact if misuse occurs and limits unnecessary access.
Weak technical safeguards	High technical-control gap	Improve multi-factor authentication, monitoring coverage, encryption, and privileged access review	Reduces opportunity and improves detectability.
Organizational pressure	High workload or unclear role score	Review workload allocation, clarify responsibilities, improve communication and escalation channels	Reduces stress-related error and control bypass behavior.
Behavioral deviation	Repeated exceptions or abnormal timing	Conduct contextual managerial review, refine alert thresholds, provide targeted guidance	Improves early intervention without assuming malicious intent.
Concentrated critical roles	High overall BRI in a small role group	Separate duties, rotate sensitive responsibilities, add peer review for high-risk actions	Prevents single-point insider exposure.

Table 6 turns analytical results into governance action. The decision mapping is deliberately specific because a score without an intervention plan has limited business value. Each action is linked to a measurable driver, which allows managers to evaluate whether mitigation actually reduces the underlying risk. For example, after implementing least-privilege controls, the organization can recalculate asset exposure and technical-control indicators. If scores do not decline, the intervention may have been poorly designed or incompletely implemented.

The framework also supports communication between technical and non-technical stakeholders. Security teams can explain risk drivers using evidence from the indicator model. Business managers can evaluate whether recommended controls are feasible in daily operations. Executives can compare the expected risk reduction of alternative investments. This shared language is one of the main benefits of treating insider threat prevention as business risk analytics rather than a specialized cybersecurity activity.

7.4 Policy and Organizational Learning Implications

Beyond immediate control improvement, the framework supports organizational learning. When risk drivers are tracked over time, managers can see whether risk reduction is achieved through durable process change or temporary compliance. If workload pressure remains high

 https://doi.org/10.63646/jbda.2024.020202

after staffing changes, the organization may need to redesign service commitments or automation support. If access review delay remains high despite policy reminders, the issue may be ownership ambiguity rather than awareness. Risk analytics can therefore reveal deeper management problems that traditional security metrics may miss.

The framework can also inform policy design. Policies should not only state what employees must not do; they should define how sensitive data access is granted, reviewed, logged, and revoked. They should clarify how exceptions are approved and how emergency access is monitored. They should specify responsibility for reviewing role changes after transfers, resignations, and project completion. An entropy-based view does not replace policy, but it shows which policy areas contribute most to residual risk.

8. Conclusion

This study developed an entropy-based decision framework for business risk analytics in insider threat prevention. The framework responds to an important gap in data-driven organizations: the need to measure and manage insider risk before a security incident occurs. Instead of relying only on post-incident detection, the framework integrates human conduct signals, organizational control conditions, technical safeguard maturity, and data asset exposure into a transparent business risk index. Entropy weighting is used to reduce arbitrary weighting and identify indicators that carry stronger discriminatory information across observations.

The simulated analysis demonstrates that insider risk is shaped by the intersection of asset criticality, access-control weakness, organizational pressure, and behavioral deviation. Data asset exposure and technical safeguard maturity were the largest weighted dimensions in the demonstration, confirming that business impact and control opportunity are central to prevention. Customer data and platform operations emerged as the highest-risk units, but for different reasons. Customer data was driven mainly by sensitive data exposure and control gaps, while platform operations was driven by workload pressure and abnormal access timing. This difference illustrates why risk scores must be decomposed into interpretable drivers.

Scenario analysis showed that targeted intervention on high-contribution indicators reduced the overall business risk index by 31.8%, while broad but unfocused controls reduced it by only 12.4%. Integrated technical and organizational prevention produced the strongest reduction, but it required greater coordination. These results suggest that organizations should first mitigate the most informative and actionable risk drivers, especially least-privilege gaps, monitoring gaps, and sensitive data exposure. Organizational interventions should then address residual risk linked to workload, communication, and process design.

The study contributes to the literature by reframing insider threat prevention as a business risk analytics problem and by demonstrating how entropy weighting can support explainable, pre-incident decision-making. It also offers practical value for executives, risk managers, cybersecurity teams, and data governance officers. The framework can be implemented with existing organizational data if appropriate privacy safeguards and governance controls are in place. Its outputs can support access review, data protection strategy, training design, workflow improvement, and executive risk reporting.

Several limitations should be noted. The demonstration uses simulated data rather than confidential records from a real organization. Future research should apply the framework to anonymized enterprise datasets under formal governance approval. The current model uses entropy weighting, but future studies could compare entropy weights with Bayesian, fuzzy,

machine learning, or multi-criteria decision methods. Additional research could also examine dynamic risk evolution, where employee roles, access privileges, and organizational pressure change over time. Finally, future work should study how employees and managers perceive the fairness and legitimacy of insider risk analytics, because prevention systems will succeed only if they are technically sound, ethically governed, and organizationally trusted.

Acknowledgement

The authors thank the anonymous reviewers for their constructive comments on the clarity, relevance, and managerial implications of this study. The authors also acknowledge the institutional research environments of Anhui University of Finance and Economics, Shandong Technology and Business University, and Henan University of Economics and Law. No external funding was received for this conceptual and simulation-based study.

Ethics Statement

This article presents a conceptual decision framework and a simulated dataset. It does not involve human participants, identifiable personal information, human specimens, animal subjects, or field research. Therefore, formal ethics committee approval was not required. The proposed framework should be implemented in real organizations only under appropriate privacy, data governance, and human review procedures.

Data Availability

No real organizational data were used in this study. The numerical values reported in the tables and figures were generated as a synthetic demonstration of the proposed method and can be reconstructed from the descriptions provided in the manuscript.

Conflict of Interest

The authors declare that they have no conflict of interest.

References

Chen, H., Chiang, R. H. L., and Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. MIS Quarterly, 36(4), 1165-1188. https://doi.org/10.2307/41703503

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548. https://doi.org/10.2307/25750690

Lu, Y., Ivanov, L. A., Wang, F., Pisarenko, Z. V., and Ye, C. (2024a). Management analytics: A bibliometric analysis. Nanotechnologies in Construction, 16(3), 257-266. https://doi.org/10.15828/2075-8545-2024-16-3-257-266

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135. https://doi.org/10.1093/cybsec/tyw001

Shannon, C. E. (1948). A mathematical theory of communication. The Bell System Technical Journal, 27(3), 379-423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

Akter, S., Wamba, S. F., Gunasekaran, A., Dubey, R., and Childe, S. J. (2016). How to improve firm performance using big data analytics capability and business strategy alignment? International Journal of Production Economics, 182, 113-131. https://doi.org/10.1016/j.ijpe.2016.08.018

Herath, T., and Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Operational Research, 196(2), 477-486. https://doi.org/10.1016/j.ejor.2008.03.036

Khatri, V., and Brown, C. V. (2010). Designing data governance. Communications of the ACM, 53(1), 148-152. https://doi.org/10.1145/1629175.1629210

Gordon, L. A., and Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457. https://doi.org/10.1145/581271.581274

Wang, T. C., and Lee, H. D. (2009). Developing a fuzzy TOPSIS approach based on subjective weights and objective weights. Expert Systems with Applications, 36(5), 8980-8985. https://doi.org/10.1016/j.eswa.2008.11.035

Gupta, M., and George, J. F. (2016). Toward the development of a big data analytics capability. Information and Management, 53(8), 1049-1064. https://doi.org/10.1016/j.im.2016.07.004

Siponen, M., and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502. https://doi.org/10.2307/25750688

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., and Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2). https://doi.org/10.1080/17517575.2024.2448003

Cheng, L., Liu, F., and Yao, D. D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), e1211. https://doi.org/10.1002/widm.1211

Ye, J. (2010). Multicriteria fuzzy decision-making method using entropy weights-based correlation coefficients of interval-valued intuitionistic fuzzy sets. Applied Mathematical Modelling, 34(12), 3864-3870. https://doi.org/10.1016/j.apm.2010.03.025

Abbasi, A., Sarker, S., and Chiang, R. H. L. (2016). Big data research in information systems: Toward an inclusive research agenda. Journal of the Association for Information Systems, 17(2), 1-32. https://doi.org/10.17705/1jais.00423

Johnston, A. C., and Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS Quarterly, 34(3), 549-566. https://doi.org/10.2307/25750691

Lu, Y., and Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847

Husak, M., Komarkova, J., Bou-Harb, E., and Celeda, P. (2019). Survey of attack projection, prediction, and forecasting in cyber security. IEEE Communications Surveys & Tutorials, 21(1), 640-660. https://doi.org/10.1109/COMST.2018.2871866

Wang, J. J., Jing, Y. Y., Zhang, C. F., and Zhao, J. H. (2009). Review on multi-criteria decision analysis aid in sustainable energy decision-making. Renewable and Sustainable Energy Reviews, 13(9), 2263-2278. https://doi.org/10.1016/j.rser.2009.06.021

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J., Dubey, R., and Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356-365. https://doi.org/10.1016/j.jbusres.2016.08.009

Puhakainen, P., and Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757-778. https://doi.org/10.2307/25750704

Kou, G., and Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1-34. https://doi.org/10.1186/s40854-024-00668-6

Buczak, A. L., and Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys and Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

Rezaei, J. (2015). Best-worst multi-criteria decision-making method. Omega, 53, 49-57. https://doi.org/10.1016/j.omega.2014.11.009

Grover, V., Chiang, R. H. L., Liang, T. P., and Zhang, D. (2018). Creating strategic business value from big data analytics: A research framework. Journal of Management Information Systems, 35(2), 388-423. https://doi.org/10.1080/07421222.2018.1451951

Vance, A., Siponen, M., and Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information and Management, 49(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Chen, Y., Lu, Y., Bulysheva, L., and Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. https://doi.org/10.1007/s10796-022-10248-7

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., and Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7, 41. https://doi.org/10.1186/s40537-020-00318-5

Rezaei, J. (2016). Best-worst multi-criteria decision-making method: Some properties and a linear model. Omega, 64, 126-130. https://doi.org/10.1016/j.omega.2015.12.001

Muller, O., Fay, M., and vom Brocke, J. (2018). The effect of big data and analytics on firm performance: An econometric analysis considering industry characteristics. Journal of Management Information Systems, 35(2), 488-509. https://doi.org/10.1080/07421222.2018.1451955

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse. Information Systems Research, 20(1), 79-98. https://doi.org/10.1287/isre.1070.0160

Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215-234. https://doi.org/10.1007/s10796-021-10221-w

Chandola, V., Banerjee, A., and Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1-58. https://doi.org/10.1145/1541880.1541882

Zadeh, L. A. (1965). Fuzzy sets. Information and Control, 8(3), 338-353. https://doi.org/10.1016/S0019-9958(65)90241-X

Gunther, W. A., Rezazade Mehrizi, M. H., Huysman, M., and Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. Journal of Strategic Information Systems, 26(3), 191-209. https://doi.org/10.1016/j.jsis.2017.07.003

D'Arcy, J., Herath, T., and Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. Journal of Management Information Systems, 31(2), 285-318. https://doi.org/10.2753/MIS0742-1222310210

Zhang, C., and Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224

Ahmed, M., Mahmood, A. N., and Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31. https://doi.org/10.1016/j.jnca.2015.11.016

Bellman, R. E., and Zadeh, L. A. (1970). Decision-making in a fuzzy environment. Management Science, 17(4), B141-B164. https://doi.org/10.1287/mnsc.17.4.B141

Janssen, M., van der Voort, H., and Wahyudi, A. (2017). Factors influencing big data decision-making quality. Journal of Business Research, 70, 338-345. https://doi.org/10.1016/j.jbusres.2016.08.007

Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660. https://doi.org/10.1111/j.1540-5915.2012.00373.x

Lu, Y. (2019). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1-29. https://doi.org/10.1080/23270012.2019.1570365

Sommer, R., and Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy, 305-316. https://doi.org/10.1109/SP.2010.25

Saaty, T. L. (1977). A scaling method for priorities in hierarchical structures. Journal of Mathematical Psychology, 15(3), 234-281. https://doi.org/10.1016/0022-2496(77)90033-5

Chen, Y., Ramamurthy, K., and Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? Journal of Management Information Systems, 29(3), 157-188. https://doi.org/10.2753/MIS0742-1222290305

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information and Management, 48(7), 296-302. https://doi.org/10.1016/j.im.2011.07.002

Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of

Industrial Information Integration, 6, 1-10. https://doi.org/10.1016/j.jii.2017.04.005

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., and Inacio, P. R. M. (2014). Security issues in cloud environments: A survey. International Journal of Information Security, 13, 113-170. https://doi.org/10.1007/s10207-013-0208-7

Triantaphyllou, E., and Lin, C. T. (1996). Development and evaluation of five fuzzy multiattribute decision-making methods. International Journal of Approximate Reasoning, 14(4), 281-310. https://doi.org/10.1016/0888-613X(95)00119-2

Moody, G. D., Siponen, M., and Pahnila, S. (2018). Toward a unified model of information security policy compliance. MIS Quarterly, 42(1), 285-311. https://doi.org/10.25300/MISQ/2018/13853

Xu, L. D., Lu, Y., and Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. https://doi.org/10.1109/JIOT.2021.3060508

Zissis, D., and Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592. https://doi.org/10.1016/j.future.2010.12.006

Wu, J., Sun, J., Liang, L., and Zha, Y. (2011). Determination of weights for ultimate cross efficiency using Shannon entropy. Expert Systems with Applications, 38(5), 5162-5165. https://doi.org/10.1016/j.eswa.2010.10.046

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers and Security, 31(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers and Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003

Lu, Y., Pisarenko, Z. V., Yang, L., and Ye, C. (2024b). Advancing decision-making: The role of management analytics in modern business practices. Nanotechnologies in Construction, 16(5), 431-440. https://doi.org/10.15828/2075-8545-2024-16-5-431-440

Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207

Opricovic, S., and Tzeng, G. H. (2004). Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS. European Journal of Operational Research, 156(2), 445-455. https://doi.org/10.1016/S0377-2217(03)00020-1

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. (2013). Future directions for behavioral information security research. Computers and Security, 32, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. Computers and Security, 32, 242-251. https://doi.org/10.1016/j.cose.2012.10.003

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876-1907. https://doi.org/10.1080/17517575.2021.2008513

Craigen, D., Diakun-Thibault, N., and Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10), 13-21. https://doi.org/10.22215/timreview/835

Mardani, A., Jusoh, A., Nor, K. M. D., Khalifah, Z., Zakwan, N., and Valipour, A. (2015). Multiple criteria decision-making techniques and their applications: A review of the literature from 2000 to 2014. Economic Research-Ekonomska Istraživanja, 28(1), 516-571. https://doi.org/10.1080/1331677X.2015.1075139

Da Veiga, A., and Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers and Security, 49, 162-176. https://doi.org/10.1016/j.cose.2014.12.006

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., and Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Computers and Security, 116, 102644. https://doi.org/10.1016/j.cose.2022.102644

Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., and Burnap, P. (2020). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial

intelligence in the industrial Internet of Things and Industry 4.0 supply chains. Cybersecurity, 3, 13. https://doi.org/10.1186/s42400-020-00052-8

Kahneman, D., and Tversky, A. (1979). Prospect theory: An analysis of decision under risk. Econometrica, 47(2), 263-291. https://doi.org/10.2307/1914185

Mady, A., Gupta, S., and Warkentin, M. (2023). The effects of knowledge mechanisms on employees' information security threat construal. Information Systems Journal, 33(3), 790-841. https://doi.org/10.1111/isj.12424

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire. Computers and Security, 42, 165-176. https://doi.org/10.1016/j.cose.2013.12.004

Casino, F., Dasaklis, T. K., and Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Saberi, S., Kouhizadeh, M., Sarkis, J., and Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117-2135. https://doi.org/10.1080/00207543.2018.1533261

Bertino, E., and Sandhu, R. (2005). Database security: Concepts, approaches, and challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), 2-19. https://doi.org/10.1109/TDSC.2005.9

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Role-based access control models. Computer, 29(2), 38-47. https://doi.org/10.1109/2.485845

Hu, V. C., Kuhn, D. R., Ferraiolo, D. F., and Voas, J. (2015). Attribute-based access control. Computer, 48(2), 85-88. https://doi.org/10.1109/MC.2015.33

Kayes, A. S. M., Kalaria, R., Sarker, I. H., Islam, M. S., Watters, P. A., Ng, A., Hammoudeh, M., Badsha, S., and Kumara, I. (2020). A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues. Sensors, 20(9), 2464. https://doi.org/10.3390/s20092464

Kamatchi, K., and Uma, E. (2025). Insights into user behavioral-based insider threat detection: Systematic review. International Journal of Information Security, 24, 88. https://doi.org/10.1007/s10207-025-01002-6

Yi, J., Song, D., and Lee, S. (2024). Insider threat detection model enhancement using hybrid supervised learning and unsupervised outlier scoring. Electronics, 13(5), 973. https://doi.org/10.3390/electronics13050973

Mladenovic, D., Stankovic, S., and Vasiljevic, M. (2024). Sentiment classification for insider threat identification. Scientific Reports, 14, 26280. https://doi.org/10.1038/s41598-024-77240-w