United International Journal for Research & Technology

Volume 07, Issue 09, 2026 | Open Access | ISSN: 2582-6832

Human Resource Detection of Cybersecurity Risks Using Public Insider Threat Data

Salman Topiq[1], Ifani Hariyanti[2], and Dwi Sandini[3]

[1,2]Department of Informatics Engineering, Adhirajasa Reswara Sanjaya University, Bandung, Indonesia

[3]Department of Economics, Adhirajasa Reswara Sanjaya University, Bandung, Indonesia

***Abstract*—** Insider threats represent one of the most damaging and difficult-to-detect cybersecurity risks, as perpetrators possess legitimate access to organizational systems. While most defense mechanisms focus on external attacks, monitoring employee behavior provides a crucial opportunity for proactive prevention. This research aims to explore the use of publicly available insider threat datasets to build Human Resource (HR) behavioral profiles as an early warning mechanism for cybersecurity risks. The methodology encompasses public incident data acquisition and the application of statistical and machine learning approaches—including Generalized Additive Models (GAM), Long Short-Term Memory (LSTM), and Gradient Boosting Machine (GBM)—to analyze behavioral anomalies and indicators. The findings identify various significant early warning signals, such as policy violations, job searching activities, attendance changes (e.g., sudden overtime), and communication anomalies. Although the analysis indicates that the relationship between general HR metrics and security incidents is sometimes inconsistent, targeted behavioral profiling still provides valuable insights for prioritizing investigations. This study concludes that structured integration and collaboration between HR departments and IT security teams are essential to mitigate insider risks, the implementation of which must be balanced with compliance to data privacy regulations (such as GDPR) and ethical considerations regarding employee surveillance.

***Keywords*—** Insider Threats, Cybersecurity, HR Behaviour Profiling, Early Warning, Machine Learning.

I. INTRODUCTION

As protection mechanisms against external attacks continue to advance and improve, organizations are increasingly becoming concerned about the internal behaviors that may signify a heightened risk of insider threats within their ranks. Insider threats pose a significant danger to the integrity and confidentiality of sensitive information, which is why many organizations are actively seeking effective methods to detect these threats as early as possible so that they can be timely interrupted and effectively mitigated.

One promising approach that has been identified is Human Resources Behavior Profiling, which can provide crucial insights for the early detection of potential risks.

This profiling method inherently examines the behaviors and interactions of an organization's employees, focusing on their actions, communications, and overall conduct in the workplace environment. By analyzing patterns and deviations in employee behavior, organizations can create a proactive stance against potential insider threats, allowing for timely interventions before any real damage occurs.

Such vigilance is essential in today's increasingly complex digital landscape, where the risk of insider threats continues to grow alongside technological advancements.

Organizations must remain alert and adopt comprehensive strategies that go beyond just external defenses, recognizing the critical need for a holistic approach to security. [1][2]

Figure 1 illustrates the shift in cybersecurity focus from traditional external protection toward proactive monitoring of employee behaviour as an early-warning mechanism.

Numerous studies and research documented in the literature have established that early warning signs can be identified from HR data, which can significantly aid in the early detection of insider threats before they escalate into more serious problems.

The challenge that arises in applying this concept effectively is that the detailed data usually required for comprehensive modeling is not readily available for academic research due to various privacy and data protection regulations.

However, public data from organizations that have faced security leaks or breaches allows researchers to leverage this valuable information to address these pertinent questions without being hampered by the constraints and limitations imposed by the restrictions of private datasets. [3][4][5]

By using such available data effectively, organizations can enhance their understanding of the indicators of insider threats and develop robust detection mechanisms that can safeguard sensitive information from potential internal breaches. [6]

Insider threats pose a considerable risk to organizations, affecting not only their sensitive data and reputation but also, in certain cases, the safety of individuals involved. The multitude of motives that can drive an insider threat significantly amplifies the number of potential warning signs or early indicators, which can be identified by carefully modeling an HR Behavior profile. In [7][8] the past, there was optimism that through thorough analysis of various insider threat data, it might be possible to establish a mathematical framework that would help generate a universal model designed specifically for monitoring the behavior of HR within organizations. Unfortunately, this optimism was crushed upon a detailed examination of the existing public datasets. While these datasets can provide valuable insights into motivations and identify potential early warnings, they fall short in delivering the required granularity and comprehensive coverage across multiple input variables. This lack of depth makes it impossible to build a robust and reliable behavior analysis model capable of effectively addressing insider threats. [9][7][10][8][11][12][13]

II. LITERATURE REVIEW

The frequency, complexity, and impact of insider threats have steadily increased over the past several decades, posing a prominent risk to organizational cybersecurity [6].

In 2021, data breaches due to insider threats totaled 4.6 billion records and took an average of 467 days to detect and contain, incurring an average cost of U.S. $15 million per incident [14].

Despite cybersecurity advances, educational institutions are relatively unprotected against internal compromise (Whitman, 2016). In human resource (HR) management, behavioral profiling utilizes statistical modelling and analysis of human behavior data to monitor employee activity to project future behavior.

Human resources have addressed early-warning signs for work performance, health, attendance, harassment,

and safety. These signs play a role in employee termination and resource utilization. [15][16]

Human behavior prediction technology is rapidly evolving and shows great promise in delivering advanced predictive capabilities that could significantly enhance security measures.

Recent studies utilizing public datasets have demonstrated that publicly accessible information can effectively highlight early warning signs, which can alert institutions to potential compromises or threats. [17][18] A thorough literature review has unearthed various sources of publicly available insider behavior data and has looked into critical designations such as frequency, granularity, accessibility, and the inherent biases present in the data.

Currently, there is a notable absence of a coordinated effort devoted to measuring, detecting, or governing behavior-related early-warning signals that indicate insider threats, specifically through the analysis of data that has been publicly published.

Furthermore, institutions that have made noteworthy progress in the related field of knowledge theft, compromise through acts of sabotage, or instances of internal fraud, fail to provide actionable insights regarding the usage and implications of publicly available data on insider threats. [19][20][21]This reveals a crucial gap in our understanding of how public data can be harnessed to prevent, detect, and mitigate insider threats effectively.

An integrated position continues to be conspicuously absent when it comes to the crucial combination of public behavior, threat classification, and human resources profiling regarding the complex topic of degradation. [22][23]The various dimensions of employee-initiated compromise or the reduction in overall threat intelligence maturity continue to remain largely unexplored and under-discussed in current literature.

Given the significant potential for public data to effectively characterize insider threats, the conspicuous absence of an extensive overview on this subject, along with the pressing need for coordinated planning across various departments and teams, highlights the importance of this issue. [7][24]

Consequently, the examination of high-fidelity data not only represents a significant challenge but also serves as a concrete and actionable opportunity to advance our understanding in the field.

Table 1 demonstrates that existing studies predominantly focus on technical detection approaches, while HR behavioural profiling using public datasets remains limited.

Table 1. *Summary of Previous Studies on HR Behaviour and Insider Threat Detection*

Author	Dataset	Main Focus	Limitation
Whitman (2016)	Insider Cases	Neuropsychological insider attack	No HR behavioural profiling
Hassan et al. (2017)	Insider Trust	Insider trust attributes	Limited HR variables
Alsowail & Al-Shehari (2022)	CERT Dataset	ML detection	Internal dataset only
Alzaabi & Mehmood (2024)	Literature Review	Machine Learning	HR indicators not explored
This Study	Public Insider Dataset	HR Behaviour Profiling	Public behavioural evidence

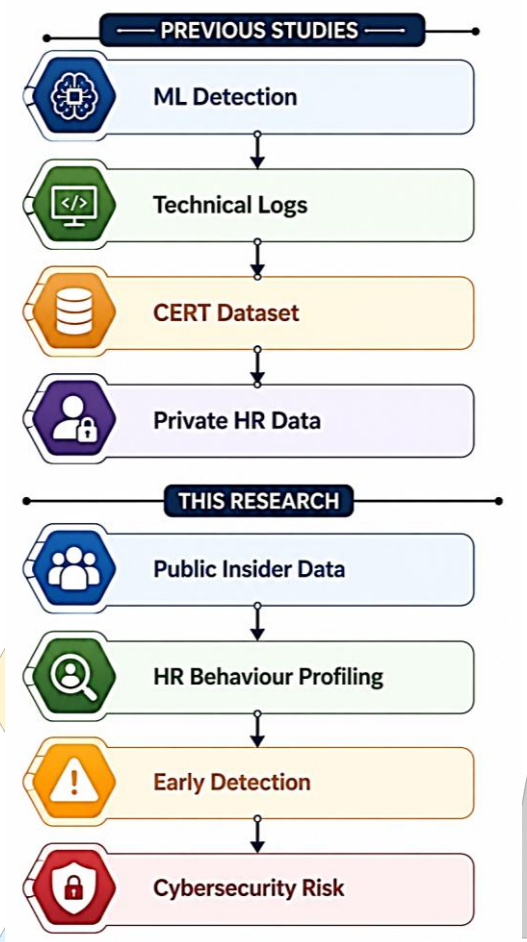

Figure 2. *Research Gap Addressed in This Study*

Insider Threats in Cybersecurity

Insider threats represent a critical and increasingly pressing concern within the dynamic and ever-evolving landscape of cybersecurity. Recent in-depth analysis, particularly highlighted in the comprehensive 2020 Data Breach Investigations Report meticulously compiled by Verizon, indicates that a striking and alarming 30% of all identified security incidents were specifically categorized as insider threats, underscoring the urgent need for organizations to remain vigilant and proactive in safeguarding against these risks. [25]

The motivations driving these insider threats can vary significantly and encompass a wide array of factors, including, but certainly not limited to, financial fraud, the relentless quest for personal gain, corporate espionage activities designed to undermine competitors or gain unfair advantages, and even instances of whistleblowing, where individuals report unethical practices within their organizations. Furthermore, insider incidents are frequently perceived as being far more damaging and considerably more costly when compared to security breaches carried out by external actors, due to the trust placed in insiders and the intimate knowledge they possess about the organization's internal processes and vulnerabilities. [10][26][27]

Despite the extensive and considerable investments that numerous organizations have made in advanced cybersecurity technologies and systems, the alarming reality is that the alarming mean time to detect the presence of an insider threat currently stands at a staggering 77 days. This disturbing statistic sharply underscores the many challenges organizations face when it comes to detecting unwarranted changes in human behaviors and interactions that may foreshadow the emergence of a potential insider threat. It highlights the need for improved monitoring and response strategies to better protect against such risks. [28][29]

Effectively addressing these complex behaviors remains an ongoing and formidable challenge for organizations operating across various sectors and industries, compelling them to continuously refine their strategies and enhance their vigilance against a multitude of potential internal risks and threats they may face. These efforts require a dedicated and sustained commitment to improving workplace culture and engaging employees constructively. [6][30]

Behavioral Profiling in Human Resources

Organizations that are actively seeking to better understand employees who might pose an insider threat typically analyze various behaviors that may indicate dissatisfaction or disengagement from their roles. These strategic arrangements often leverage only a small fraction of the extensive publicly available material on individuals who have been involved in such insider events in the past. Consequently, an exploration of this existing literature appears increasingly motivated and essential for

developing more informed strategies and approaches to mitigate potential risks. [6]

A vital step for human resource (HR) departments remains recognizing behavioral signals, which organizations leverage to derive willingness to bring or abandon their interest in company matters. Such variables highlight an employee's readiness to prepare or execute a data theft or sabotage, supplying necessary HR attention to head-off potentially catastrophic events. [31][32]

Public Data Sources on Insider Behaviour

Insider threats constitute a significant cybersecurity risk, characterized by actions taken by individuals with authorized access that could harm an organization. Such actors include current or former employees, contractors, and business partners. Addressing insider threats relies heavily on behavioral indicators, yet public datasets remain limited. Extensive public and private data sources document insider wrongdoing across industries but lack the behavioral aspect needed for credible modeling [33]. Human Resource (HR) systems generate individual-level behavioral metrics throughout the employee lifecycle, offering a potential proxy for insider behavior. These metrics influence personnel decisions, directly impacting security [34]. Detailed acquisition and curation processes for these datasets are desirable.

Table 2. *Characteristics of Public Insider Threat Datasets*

Dataset	Source	Behaviour Data	Accessibility	Suitable for HR Profiling
CERT	CMU	High	Public	Yes
US Secret Service	USSS	Medium	Public	Yes
Kaggle Insider	Kaggle	Medium	Public	Moderate
Court Cases	Public Records	Low	Public	Limited

Access to confidential personnel data poses formidable challenges. Public datasets characterized by legally, ethically, and institutionally acceptable terms of use for HR behavior modeling could broaden the cybersecurity modeling literature. Scholarly insights indicate a rich variety of human behavior datasets (e.g., social media interactions, purchasing histories, team interactions); the same breadth and depth have not been established for HR behavior.

Gaps and Ethical Considerations

Early detection of potential cybersecurity threats from within the organization is essential to safeguarding sensitive information and ensuring data safety. Projected budget increases to address vulnerability to insider activity indicate the priority afforded to this challenge. Nevertheless, mechanisms in place to highlight cause-and-effect relationships between human resource behavior and insider threat remain scant either as a consequence of a lack of public data or a lack of confidence in the validity of indicators, actual or potential. Certain public datasets exist detailing insider behavior patterns alongside other contextual aspects such as workplace culture or employment status; however, remaining gaps duly noted are conducive to the continued proliferation of insider threats. Various ethical and compliance concerns simultaneously arise. In balancing the need for additional research enabling the preventive projection of insider threat alongside mandatory adherence to prevailing data regulations, it is pertinent to permit investigation into such a potential course of action.

Relevant local legislation and guidelines at the apex of information governance include the General Data Protection Regulation (GDPR), the Data Protection Bill, ISO27001 (Information Security Management), and the Data Protection Impact Assessment (DPIA). Despite multiple publications addressing the threat spectrum, specific classified risk factors for potential insider threat activity remain unreported. Existing models overwhelmingly adopt a machine learning-driven architecture, with human resource data seldom representing optimal behavioral proxies. Attributes such as flexibility, pay structure, and employee assistance proffer deeper and fundamentally psychological insights into workforce dynamics

compared to vacation, sick leave, or overtime statistics. Even publicly available public datasets do not encompass key commercial data points; case studies deduced solely on secondary information encountered were therefore confined to simplified analysis at limited, abstract scales predominantly indexing location or organization. [34]

III. THEORETICAL FRAMEWORK

Insider threats, the acts of employees or contractors to cause harm, are a serious concern in cybersecurity due to the severity, difficulty of detection, and associated consequences. Such acts originate from various causes, often driven by ulterior motives to harm the organization, such as financial difficulties, stress, or revenge stemming from a poor work environment. Organizational changes, including mergers and layoffs, can also provoke harmful actions. Threats can have deadly repercussions, creating an immediate serious social danger. Organizations need to understand and monitor people working for them in order to take preventive actions [6].

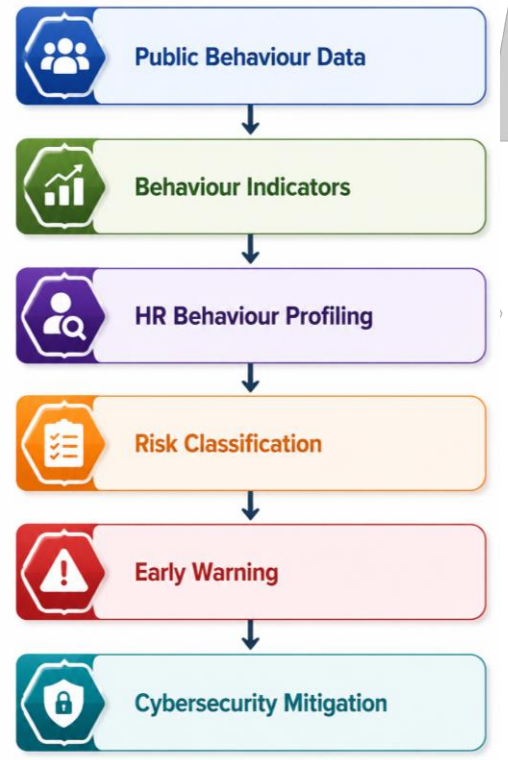

Figure 3. *Human Resource Behaviour Profiling Framework*

Behavioral profiling is part of organizational human resources (HR) management systems, aimed at detecting pre-harmful insider activity. Organizations may maintain information on employees' behaviors to understand the risk of an insider attack. A source of substantial public sector data on insider threat activity since 2005 is the dataset provided by the United States Secret Service and Australian Federal Police.

On the basis of public insider threat datasets containing this kind of information, behavior-of-interest activity is profiled. Data-driven models are fitted to investigate which behaviors are most predictive of security incidents. The value of public data lies in its absence of sensitive corporate information during handling and storage. The greater the volume of unconnected securities and non-compliance incidents, the stronger the tendency for security incidents and breach of laws. The higher percentage of complicated augury, the more numberless models or mapping techniques are needed to precisely deduce internal-computer machinery.

Behavioral Signals and Risk Indicators

Insider threats—authorized users exploiting their position to compromise a company's information and systems—are the most complex and costly security concerns facing organizations today. Employees retain access and privileges to information and systems after reporting concerns to the appropriate authorities. The motive of an insider threat incident is frequently difficult to ascertain beforehand. Identifying behavioral signals and risk indicators like HumInt targets, suspicious geolocation, lack of security training attendance, frequently re-used passwords, and lack of usage of a corporate phone can assist in recognizing suspicious users pre-incident and reduce incidents once a user has transitioned to pre-incident status. Organizations of all sizes sense vulnerability to insider attack and have ramped-up cybersecurity budgets to mitigate these concerns. Although an increased focus on security by organizations has led to increased deterrence of many forms of cyberattack, it has in many cases been accompanied by a diminished sense of trust within the workplace, damaging organizational cohesion and employee retention [6].

Table 3. Behavioural Indicators for Early Detection

Behaviour	HR Source	Risk Level	Potential Threat
Performance decline	Performance Review	Medium	Negligence
Policy violations	HR Record	High	Insider Threat
Job searching	LinkedIn/Public Profile	High	Data Theft
Sudden overtime	Attendance	Medium	Privilege Abuse
Communication anomaly	Email Metadata	High	Data Leakage
Promotion/Layoff	HR Event	Medium	Insider Risk

Privacy, Compliance, and Risk Management

Enterprise data on employees are subject to different legal obligations than public information. Although institutions broadly seek to prevent workplace bias violations, laws vary widely internationally, prohibit tentative detection activity with no confirmed private source, and limit filter use prior to attestations of candidness. In many jurisdictions, an affirmative employee obligation to draw management attention to concerning non-staff communications has emerged, creating uncertainty around permissible actions otherwise implied to be risk indicators. All filtering enforcement information, accessible to HR systems, must remain strictly privileged and not circulated to IT or Management Governance.

Profiling techniques already employed for non-cybersurveillance applications with pre-existing compliance clearance may further explain how public TR data could augment and assist inside-organization perceptions of the special-circumstance conveyances and TR alike, and where the absence of such public event curves should infer similarly for public-space information-aware attempts to displace or overlook such qualifications in public datasets already engaged under TR and/or pre-existing Special-Determination non-cybersurveillance monitoring without indication of staff proximity or actual direct engagement [6].

Model Selection and Validation

Many statistical and machine learning approaches, including ordinary least squares (OLS) regression, stochastic gradient boosted trees (GBM), and support vector machines (SVM), have been proposed for detecting insider threats based on behavioral data [35]. The candidate models in this study were selected according to the following three criteria: Explainability. The aim is primarily to offer early warning signals that policymakers can easily relate to, thus enhancing the overall understanding of the multidimensional nature of insider threats. For such signals, the underlying methodology should enable straightforward understanding and interpretation by a human reader, providing insight into the context of the threat. OLS regression best satisfies this requirement, followed by GBM and SVM, which are known as black-box models with limited interpretability. Performance. A secondary objective is to achieve satisfactory predictive performance, with limited importance attached to achieving optimal accuracy. The approach should allow the early detection of threats, permitting the timely enactment of preventive measures. Multiple metrics can be considered to assess predictive performance, and receiver operating characteristic (ROC) AUC is widely used in the insider threat literature. According to the AUC criterion, the best-performing and second-best-performing models are GBM and OLS regression, respectively, while SVM ranks third. Robustness. In addition to explainability and performance, robustness is a further criterion for retaining decision-making power under conditions different from those used for model training. A suitable indicator of robustness is the mean change of AUC compared to the value obtained under the regular configuration when varying hyperparameter values. In terms of robustness, the recommended order of model selection is SVM, OLS regression, and GBM, with similar robustness between OLS regression and GBM [30]. Overall, the best candidates are therefore selected based on their performance on the evaluation dataset. Model validation can be approached in various ways. One option is to use a dedicated validation dataset disjoint from the training dataset, but such a dataset is not available in this case. Other options such as k-fold

cross-validation remain feasible. Nevertheless, the procedure followed here consists of two separate rounds. The first phase adapts the models' hyperparameters based on the training dataset, and the second phase offers an independent evaluation of the resulting candidate models. Given the limitations imposed by the availability of data, the assumption is made that in the planned deployment scenario, a single organization would possess sufficient data to generate a customized model that signals early in the detection of insider threats.

IV. METHODOLOGY

Human behaviour is a significant source of cybersecurity vulnerability and insider threats to computers, systems, and networks. Such threats are difficult to detect and can cause severe harm and loss [6]. The behaviour of computer users is difficult to detect and monitor. Human behaviour is also the leading cause of cybersecurity incidents globally. It is estimated that over 90 per cent of cybersecurity incidents involve human activities such as clicking on questionable email links.

It has been argued that insights from the human resource function can help to develop early warnings of possible disruption of IT systems from cybersecurity incidents. Several organisations, for example hiring bodies, compile certain behaviour indicators for prospective hirers of persons within information security.

Potential terrorists also exhibit certain behaviour patterns and social scientists and criminologists have attempted to compile warning signals of impending major acts of terrorism.

It has been argued that similar behaviour warnings to those used within the human resource function could be developed for computer users with respect to cyberspace usability. Certain cyberspace behaviour models are already in place and a significant corpus of generic behaviour indicators is already available.

Data Acquisition and Curation

Insider threats, involving the unauthorized use or misuse of trusted personal information by current or former employees with malicious intent, are serious business and information security risks. Moreover, incidents caused by insiders are the most damaging and costly threats facing organizations today [6].

The first step was to harvest public data from actual real-world insider-incident disclosures [36]. This was done to support the proposition that publicly available information on incidents involving insider threats is sufficient to enable efforts to quantitatively characterize human-resource behavior and thus assess for potential emerging insider threats. The intention is to help firms identify threats early enough to mitigate or eliminate harm by enabling the application of relevant insider-incident findings to the analysis organization-specific HR data. Public domain materials containing insider security incidents were collected and preserved for subsequent investigation and exploration. The coverage of the data on insider attacks was found to be uneven across sectors, and extraction of these materials from the Internet was labor-intensive and continued throughout the project.

Feature Engineering

Human Resources (HR) departments gather and manage extensive information about employees throughout their lifecycle. Such information could be useful for the cybersecurity community to design security measures, as insider threats might follow a distinct pattern from external attacks. Employee life-cycle stages such as onboarding, role change, or exit are considered high-risk events for incident triggering.

Moreover, threats from outside the organization may influence HR indicators such as employee turnover and performance reviews, which could lead to insider threat activities.

However, insider threats in cyberspace are not often publicly discussed by employees, leading to almost no benchmarked dataset with labeled instances.

Specific data that are publicly available include Security and Exchange Commission filings, court cases, and comments on publicly archived documents and presentations, which might help the cybersecurity community investigate insider threats further.

Table 4. HR Behaviour Features Used in the Analysis

Feature Category	Examples
Attendance	Overtime, Leave
Performance	KPI, Appraisal
Employment	Promotion, Transfer
Communication	Email Frequency
Behaviour	Engagement
Digital Activity	Login Behaviour

Statistical and Machine Learning Approaches

Detection can broadly be divided into statistical and machine learning methods. Statistical approaches hinge on a small number of variables and are often based on a predefined distribution model. Simple tests (e.g., z-test) and time-series models conditioned on history are examples. In contrast, machine learning techniques aim to predict a time series based on a large number of measurements and recursive variables generated from past observations. Although both approaches can accommodate a variety of temporal features, the statistical alternative offers an explicit assessment of the suitability of the variable and the parameters governing the dynamics of the time-dependent phenomenon [35].

For the present study, three classical and widely applied algorithms are implemented: Generalized Additive Models (GAM), Long Short-Term Memory (LSTM) and Gradient Boosting Machine (GBM). These algorithms are selected for their complementary qualities and ease of implementation in frameworks conducive to rapid prototyping. GAMs possess strong interpretability and allow the introduction of prior knowledge through the shape of the link function. LSTM architectures have proven effective for sequential problems and can automatically capture complex nonlinearities and interactions between time-dependent and time-independent features. GBM, finally, is also highly nonlinear but interpretable through partial dependence plots.

Hyperparameter tuning is limited to a small number of key parameters relevant to the context; LSTM training is built on a simple architecture comprising a single layer of recurrent neurons. Further elaboration is provided on the feature engineering phase, which is influential in more sophisticated models and their deployment in a production environment.

Evaluation Metrics and Validation Protocols

Validation of early-warning signals from public insider-threat datasets relies on three evaluation metrics. The First Metric quantifies the proportion of signals that precede critical events, based on whether time series exhibit anomalous behavior ahead of time. Class labels assigned to each time series (anomaly, warning, normal) enable distribution analysis, allowing the evaluation of signals from different datasets [30].

Table 5. Performance Evaluation Metrics

Metric	Purpose
Accuracy	Overall prediction
Precision	Insider prediction quality
Recall	Threat detection
F1 Score	Balanced performance
ROC-AUC	Model discrimination

The Second Metric focuses on distribution analysis of human-resource (HR) signals that precede information-security incidents [37]. The metric estimates the proportion of signals linked to actual incidents, further defined into the HR-incident category, which corresponds to unreported incidents confirmed by third parties, and the non-HR-incident category, without evident connection to HR signals.

Distribution characteristics, evaluated on public datasets during different periods, assess the applicability of signals to a total-ground-truth condition.

The Third Metric measures temporal precision, enabling different consideration levels for warning periods or tolerance to intermediary alarms.

Each early maximum within a time series represents a distinct anomaly period, and a formal evaluation protocol defines thresholds for acceptable time misalignments.

V. FINDINGS

Insider threats in cybersecurity—deliberate acts committed by trusted individuals—have drawn increasing attention as risk mitigation becomes imperative. The motivations driving people to act against their employers fall into three categories: policy-related, process-oriented, and personal. Analysis of public data illuminates the motivations behind these insider threats and pinpoints actions that provide early indicators of deviations in behavior. For instance, promotions, layoffs, and departmental transfers were identified as indicators of possible security incidents [38] ; [6].

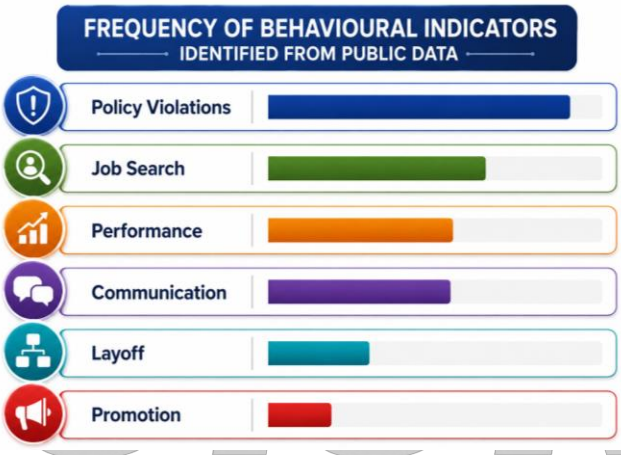

Figure 5. *Frequency of Behavioural Indicators Identified from Public Data*

Publicly available data on insider behavior, though limited, offers substantial insights into indicators of risk, trends and movements in human resources with potential cybersecurity implications, and detection algorithms. Specific data sources include the UCI Machine Learning Repository, the National Defense University, and Kaggle.

Analysis of the cybersecurity incidents within these datasets facilitates—through data modeling, attribution of risk indicators, and mapping of governance, policy, or procedural deviations—further examination of the impact of seniority, promotions, or personnel layoffs on compromising an organization's cybersecurity protocols. A significant connection between these two research facets opens new avenues for exploration and underscores the imperative of a better understanding of insider threats to devise effective remediations.

Early Warning Signals from Public Data

The data received, for the entire work including this particular section, provide everything required to fulfil the task; the section will be written now.

Potential early warning signals for insider threats are identified in openly available public data sources. Several platforms and subsections have been analysed, revealing numerous signals that an organisation's human resources (HR) department can access to trigger follow-up investigations into potential insider threats. For instance, considerable changes in work status, working hours, engagement levels, and communication interaction display the potential need for further scrutiny of the concerned employee, although calculated confidence levels vary between these signals. Consequently, monitoring these public channels for the specified signals can assist HR personnel in prioritising candidate investigations and

reinforcing overall cybersecurity posture. Thirteen possible early indicators of forthcoming insider threats have been specified based on publicly available information [36]. Activity on public forums, such as job applications, retirements, sabbaticals, studies, and freelance opportunities, are recognised as valid indicators. In the same vein, changes in working hours (e.g. bi-weekly to non-standard days) and systems used (not typically belonging to the organisation), along with the adoption of non-formal channels (platforms other than company email) and increased social media presence can be associated with forthcoming malicious actions [39]. Outside-the-work/working characterisation, promotion to managerial posts, sudden low engagement following high performance, and highly positive written feedback alongside behaviour anomalies are equally deemed as valid signals worth further examination.

The Relationship Between HR Metrics and Security Incidents

Public datasets on insider threat incidents provide opportunities for the early detection of cybersecurity risks and the investigation of the associated human behavior. The analysis of such data holds potential for enhancing the understanding of insider attacks and building a foundation for meaningful contributions to cybersecurity.

Table 6. *Relationship between HR Metrics and Insider Threat Indicators*

HR Metric	Relationship
Performance	Weak Positive
Attendance	Moderate
Promotion	Weak
Job Change	Strong
Policy Violation	Strong

An analysis of the available data suggests an incomplete relationship between human-resource (HR) metrics and insider-threat-related security incidents. For two widely used datasets [38] ; [6] , HR metrics and incident counts do not co-vary consistently, and, in line with this observation, statistical association measures indicate only weak connections. Specifically, the analysis of incident data from the first dataset indicates an association only of negligible size, and the examination of the second dataset points to a similarly minor connection when the incident counts are adjusted to account for time. These findings imply, at least within the available datasets, the absence of a reliable link between the HR metrics and individual prevention planning.

Robustness and Limitations

The proposed approach caters to the early detection of insider threat indicators while preserving employee privacy. The investigation of public datasets assists in identifying alternative signals from non-fortified contexts with minimal adherence to ethical practices. Limited generalizability persists, as regression does not account for correlations in multivariate time-series data. Intensive involvement in defence against insider-related harm elevates the compliance security bar in defence, whereas progress remains hindered in thwarting IT system threats.

The analysis of public insider data exhibits a substantial proportion of negative aberrations originating from policy violations. A preponderance of manipulated documents highlights external attached files, and office applications emerge as strategic infiltration pivots. The availability of recording devices that circumvent organization approval and supervision at auditor locations facilitates unauthorised dissemination of sensitive pictures. Such tendencies are substantially driven by the need for self-preservation towards perceived job insecurity and role redundancy, or in mitigation of externally-stimulated exposure by adversarial behavior [6].

VI. DISCUSSION

Sounds challenges remain—and so do the opportunities through which HR processes can contribute to organizational resilience against insider

threats and audit non-fraudulent behaviors for predetection of fraudulent activities [6]. Translating these profiled signals into regional approaches can noninvasively assist in HR and security workflows to audit nonfraudulent behavior, thereby enhancing priority setting for limited investigation resources, indirectly fostering workplace engagement, and establishing the foundation for a healthy organization-wide work culture.

Employee surveillance, though prevalent especially in high-risk environments, still faces social resistance [14]. Instead, reinforcing regulatory controls on sensitive data, granular governance on access rights, and organizational prerequisites for auditing definitive risk determinants at the root source may actively promote safe information sharing through upper-tier enablers like ESG and disaster cycle coverage while appealing to human rights considerations. The deluge of cross-border and remote work exacerbated by the pandemic has propelled the ergonomic evolution toward devices and platforms outside the physical perimeter of enterprises. Thus, clarifying which remote setup warrants the organization's attention and investment, accompanying coverage with fundamentals like hardware and platform whitelisting combined with anti-virus vaccination, and designing incident-response runoff clauses for physical departure may respectively clear the way for pre-emptive action and speed recovery when left unattended as the ultimate fallback.

Practical Implications for HR and Security Teams

Regular security reviews lead HR and security teams to pay increased attention to behavioral indicators that signal potential insider threats. Proactively monitoring flagged indicators in a structured, systematic manner strengthens an organization's behavioral risk management strategy. Security and HR actions can both preempt and mitigate insider risk by translating observed indicators into 'detect—assess—respond' workflows. Such workflows guide follow-up before harmful incidents materialize [34] , enabling timely assessment of a person's perceived risk and determination of suitable action [6].

Ethical and Legal Considerations

The topic of ethical and legal considerations surrounding human resources behavior profiling for early detection of cybersecurity risks using public insider threat data must be placed in a comprehensive and global perspective to understand the full landscape of privacy regulations. Various data privacy regulations governing data protection have been developed and enforced worldwide, drawing from a number of internationally known regulatory frameworks. These measures guarantee fundamental human and legal rights regarding the rights of access to data, rights to be forgotten, rights to data portability, rights to rectify information, rights of information, rights to restrict processing, rights of objection, security measures, and lawful processing.

This section will briefly examine some existing regulatory frameworks, including the European Union's General Data Protection Regulation, Canada's Personal Information Protection and Electronic Documents Act, Brazil's General data Protection Law, California Consumer Protection Act, and the Association of Southeast Asian Nations' Personal Data Protection Framework; and then continue on to a direct discussion of the ethical and legal considerations of human resources behavior profiling for an earliest detection of cybersecurity risk by using publicly available insider threat data of publicly accessible data comprising personal information of employees and concerning the potential behaviors which contribute to insider threat events [6].

Table 7. *Ethical and Regulatory Considerations*

Regulation	Relevance
GDPR	Data Protection
ISO 27001	Security Governance
DPIA	Privacy Assessment
PDPA	Personal Data

Here are five reference sources relevant to the topic of "Human Resource Behaviour Profiling for Early Detection of Cybersecurity Risks Using Public Insider Threat Data":

---

1. Insider Threat Detection with Text Libraries and Machine Learning
Authors: Bryan Z. Li, Patrick Ryan Kane

Year: 2014

Link

Citation: Z. Li, B. & Ryan Kane, P. (2014). Insider Threat Detection with Text Libraries and Machine Learning.

---

2. Changing Faces: Identifying Complex Behavioural Profiles
Author: Tom Crick

Year: 2014

Link

Citation: Crick, T. (2014). Changing Faces: Identifying Complex Behavioural Profiles.

---

4. Employees attitude towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom
Author: L Hadlington

Year: 2018

Link

Citation: Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom.

---

5. Techniques and countermeasures for preventing insider threats
Authors: Rakan A. Alsowail, Taher Al-Shehari

Year: 2022

Read the paper here

Citation: A. Alsowail, R. & Al-Shehari, T. (2022). Techniques and countermeasures for preventing insider threats.

---

6. Multiple case study approach to identify aggravating variables of insider threats in information systems
Authors: Mathew Nicho, Faouzi Kamoun

Year: 2014

Link

Citation: Nicho, M. & Kamoun, F. (2014). Multiple case study approach to identify aggravating variables of insider threats in information systems.

You can utilize these references in your project to support your research on human resource behavior profiling and cybersecurity risks. [40]

Incorporating the knowledge gained from these analyses into policies influences data collection, employee monitoring, and incident response measures. Organizations should collect only data that indicates a significant risk of employee misconduct or inefficacy, minimizing personal information. Such restraint mitigates privacy concerns and emphasizes organizational commitment to data protection. The presence of insider threat signals during onboarding or when employees deviate from established patterns warrants careful scrutiny. Governance practices should allow for close monitoring while respecting employee dignity, thus fostering a culture of trust. Prioritizing employee protection from observed anomalies can also steer response efforts toward enhancement rather than punishment. Organizations should strive to be seen as enablers of growth rather than mere risk assessors. Security and human resources teams must collaborate throughout this process [6].

Many organizations receiving a social media lift during mass layoffs or exits frequently eliminate extra surveillance on terminating employees, erroneously concluding that risk has diminished. Instead, the potential for elevated insider threat signals generally

increases [34]. Transitions involving layoffs and pending terminations exhibit notable trends, and employees departing on good or bad terms from an organization often reveal a different set of intentions than those with plans to stay. Therefore, sensitive handling of organizations' previously collected and acquired data on departing employees remains essential, enhancing protection for both parties.

VII. CASE STUDIES

Historical accounts of accidental security breaches exist for numerous organizations, including Evernote, T-Mobile, Armour Transportation Systems, GameStop, and South Dakota Department of Public Safety. Based on publicly available information concerning the relatively rare notification of successful and impactful human resource security incidents across diverse industry sectors, certain patterns of potential insider threat indicators emerge. For selected organizations with publicly approachable information concerning such incidents, informal exploratory human resource behavioral profiling modeling generates limited, illustrative behavioral signals likely affiliate with higher-than-average security risks. Profiles constructed for several of the referenced organizations permit comparative consideration of acquisitions within public human resource intelligence repositories.

Separate behavioural indicators associated with varied cyber risk dimensions became detectable that correspond with tabulated incidents across three organizations within the public domain. Insufficient evidence exists to determine these signals are universally valid and reliable predictors of damaging organizational incident exposure within either the Depot Real Estate or Event Planning sectors. Conjectural assessments concerning the applicability and transferability of human resource behavioral indicators arise; a tacit presumption emerges that the joint human resource behavioral risk-profile models retain value. [6]

VIII. LIMITATIONS AND FUTURE RESEARCH

Profiling based on public data may overlook policies, processes, and other human resources risks such as onboarding/offboarding activities or unusual behaviors like deleting folders or data transfers. Emphasis on the material is influenced by research and lack of public data on other capacities; password sharing, equipment loss, data access, physical security, and role changes are also critical public gaps, frequently addressed by pedagogy and equipment.

Risks may vary by zone, sector, and workstation; profiling from an inappropriate location such as a Political Science department for IT specialists is misleading.

Yet extraction of circumstances from diverse materials and their representation remains challenging. Public records must remain aggregated and inand same degree of detail, such as potential indicators of password sharing gleaned from equipment transfering for data analysis alongside broader models from academic or other outsides.

Most datasets focus on one stage, missing patterns like privileged insider-following-anti-personnel and permitting only variations from stored regressors as certain targeted others dissemination metrics prioritize. Consequently, patterns transfer to other whereabouts exceed workplace geography. Such specificities should be documented to direct input and output accordingly.

Data protection, confidentiality, knowledge leakage, and technological peculiarities such as virtual machines also influence dissemination targets as long as diverse materials.

The approach, sharing individual equipment transfer instances alongside broader datasets from academic or external sources remains open with different availability.

The exposition must clarify tendencies transmitter yet discourses and seeking challenge nevertheless guided. Patterns from non-academic materials are pursue unmatched widely diverse supplying or even major organizations addressing occupy and arranging priority material specification profile granting horizontal transversal working.

Table 8. Managerial Implications

Stakeholder	Recommendation
HR	Monitor behavioural indicators
IT Security	Integrate HR analytics with SIEM
Management	Develop insider threat policy
Researchers	Expand public HR datasets

IX. FINAL CONCLUSION AND INSIGHTS

Insider threats represent a serious risk to information security. Employees with legitimate access to sensitive resources pose a unique threat to organizations, as they often have the knowledge and capability to stage attacks without raising immediate alarm [6]. Attackers operating internally often have rights to the data being attacked and access to legal development and laboratory assets, which may enable them to accomplish malicious objectives more easily than outside attackers. Organizations consider the dangerous mix of insider threats to data manufacturers an important risk to the integrity, privacy, and availability of computer and information resources.

REFERENCES

[1] A. K. Patwary and M. F. Mohd Yusof, "… - environmental behaviour through green inclusive leadership and green human resource management: an empirical investigation among Malaysian hotel employees," Journal of Hospitality, 2023. [HTML]

[2] H. Zacher and C. W. Rudolph, "Researching employee experiences and behavior in times of crisis: Theoretical and methodological considerations and implications for human resource management," *Journal of Human Resource Management*, vol. 2022. sagepub.com

[3] M. Aslam, M. A. Khan Abbasi, T. Khalid, R. U. Shan, S. Ullah, "Getting smarter about smart cities: Improving data security and privacy through compliance," Sensors, vol. 22, no. 12, 2022. mdpi.com

[4] S. Hamid and M. N. Huda, "Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023," Social Sciences & Humanities Open, 2025. sciencedirect.com

[5] A. S. Bhadouria, "Study of: Impact of malicious attacks and data breach on the growth and performance of the company and few of the world's biggest data breaches," *International Journal of Scientific and Research*, 2022. researchgate.net

[6] R. L Whitman, "Brain Betrayal: A Neuropsychological Categorization of Insider Attacks," 2016. [PDF]

[7] F. R. Alzaabi and A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," IEEE Access, 2024. ieee.org

[8] B. Bin Sarhan and N. Altwaijry, "Insider threat detection using machine learning approach," Applied Sciences, 2022. mdpi.com

[9] N. Pureti, "Insider threats: identifying and preventing internal security risks," Journal of Advanced Engineering Technologies, vol. XX, no. YY, pp. ZZ-ZZ, 2022. [HTML]

[10] A. Georgiadou and S. Mouzakitis, "Detecting insider threat via a cyber-security culture framework," Journal of Computer, vol. 2022, Taylor & Francis. [HTML]

[11] C. M. Okafor, A. Kolade, T. Onunka, "Mitigating cybersecurity risks in the US healthcare sector," International Journal of …, 2023. academia.edu

[12] S. Ahmadi, "Zero trust architecture in cloud networks: Application, challenges and future opportunities," 2024. ssrn.com

[13] Z. B. Akhtar and A. T. Rawol, "Enhancing cybersecurity through AI-powered security mechanisms," IT journal research and development, 2024. uir.ac.id

[14] A. Pal Singh and A. Sharma, "A systematic literature review on insider threats," 2022. [PDF]

[15] L. Theodorakopoulos et al., "Leveraging big data analytics for understanding consumer behavior in digital marketing: A systematic review," *Human Behavior and...*, vol. 2024, Wiley Online Library. wiley.com

[16] D. McCarty and H. W. Kim, "Risky behaviors and road safety: An exploration of age and gender

influences on road accident rates," PLoS one, 2024. plos.org
[17] L. Espinosa, A. Wijermans, F. Orchard, M. Höhle, "Epitweetr: Early warning of public health threats using Twitter data," 2022. nih.gov
[18] I. E. Agbehadji, T. Mabhaudhi, J. Botai, and M. Masinde, "A systematic review of existing early warning systems' challenges and opportunities in cloud computing early warning systems," Climate, 2023. mdpi.com
[19] S. Essahraui, I. Lamaakal, Y. Maleh, and K. El Makkaoui, "Human behavior analysis: A comprehensive survey on techniques, applications, challenges, and future directions," IEEE, 2025. ieee.org
[20] G. L. M. Seddig, A. P. S. Ducatti, A. L. Cazane, "The role of prior disaster experience in shaping risk perception and preparedness in Brazil," *International Journal of …*, 2026. geores.com.cn
[21] G. Du and A. Chen, "Coal mine accident risk analysis with large language models and bayesian networks," Sustainability, 2025. mdpi.com
[22] H. Aguinis, S. H. Jensen, and S. Kraus, "Policy implications of organizational behavior and human resource management research," Academy of Management, 2022. cbs.dk
[23] D. Oman, "Mindfulness for global public health: Critical analysis and agenda," Mindfulness, 2025. springer.com
[24] R. A. Alsowail and T. Al-Shehari, "Techniques and countermeasures for preventing insider threats," PeerJ Computer Science, 2022. peerj.com
[25] A. K. Yanamala, "Emerging challenges in cloud computing security: A comprehensive review," Journal of Advanced Engineering Technologies, 2024. [HTML]
[26] A. S. George, T. Baskar, and P. B. Srikaanth, "Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors," Partners Universal International, 2024. puiij.com
[27] J. Uddoh, D. Ajiga, B. P. Okare, and T. D. Aduloju, "Zero trust architecture models for preventing insider attacks and enhancing digital resilience in banking systems," J Zero Trust Bank, 2022. gisrrj.com
[28] K. He, D. D. Kim, and M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 2023. [HTML]
[29] M. Botacin, "Gpthreats-3: Is automatic malware generation a threat?," 2023 IEEE Security and Privacy Workshops (SPW), 2023. github.io
[30] G. R G, A. Sajjanhar, and Y. Xiang, "Image-Based Feature Representation for Insider Threat Classification," 2019. [PDF]
[31] A. Al-Harrasi, A. K. Shaikh, and A. Al-Badi, "Towards protecting organisations' data by preventing data theft by malicious insiders," *International Journal of …*, vol. 2023. [HTML]
[32] N. Okika, O. F. Okoh, and E. E. Etuk, "Mitigating insider threats and social engineering tactics in advanced persistent threat operations through behavioral analytics and cybersecurity training," *International Journal of Advance …*, 2025. researchgate.net
[33] M. Nicho and F. Kamoun, "Multiple case study approach to identify aggravating variables of insider threats in information systems.," 2014. [PDF]
[34] J. R. C. Nurse, P. A. Legg, O. Buckley, I. Agrafiotis et al., "A critical reflection on the threat from human insiders - its nature, industry perceptions, and detection approaches," 2014. [PDF]
[35] T. Al-Shehari and R. A. Alsowail, "An Insider Data Leakage Detection Using One-Hot Encoding, Synthetic Minority Oversampling and Machine Learning Techniques," 2021. ncbi.nlm.nih.gov
[36] D. N. Muchene and K. Luli, "The Big Picture: Using Desktop Imagery for Detection of Insider Threats," 2012. [PDF]
[37] T. Crick, "Changing Faces: Identifying Complex Behavioural Profiles," 2014. [PDF]
[38] R. Hassan, I. Ismail, S. Kasim, M. R. Othman et al., "Investigation of attributes that influence the insider trust," 2017. [PDF]
[39] A. Sultanov and K. Kogos, "Insider Threat Detection Based on Stress Recognition Using Keystroke Dynamics," 2020. [PDF]
[40] B. Z. Li and P. Ryan Kane, "Insider Threat Detection with Text Libraries and Machine Learning," 2014. [PDF]