e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 5, Issue 7, July 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

The Great Resignation: Managing Cybersecurity Risks during Workforce Transitions

Sreejith Sreekandan Nair[1], Govindarajan Lakshmikanthan[2]

Independent Researcher, Leading Financial Firm, Texas, USA[#1, #2]

ABSTRACT: Where organizations used to rely on employees tenured with their company, the Great Resignation has presented new problems to organizational structure and fortification. Such a process usually leads to disrupted employee productivity and most importantly, increased vulnerability to cyber threats. Loyal workers, intentionally or unintentionally disloyal workers, and employees who leave the organization can compromise organizational confidential information, such as innovation, customer data, and other data that the organization considers to be highly valuable. Research has also revealed that workforce transition time is also the highest-risk activity period for insiders, wherein activities like the unauthorized download of data or accidental data leaks when offboarding an employee are likely to occur. Moreover, there are difficulties, particularly for organizations that cannot apply adequate access controls and monitoring during the notice periods, making them much more sensitive to data leaks. Further, this paper examines these paramount cybersecurity threats and offers an organized framework for their mitigation. Explores how the risks can be reduced under this through policies like strong access controls, opaque data monitoring systems, and comprehensive offboarding. To get practical recommendations for managing the problem with data sharing, the example of using machine learning to realize the mechanisms for identifying anomalies and graph-theory-based mathematical models is given. Thus, this research provides a comprehensive set of procedures to address the consequences of the Great Resignation for organizations and safeguard their assets during worker turnovers.

KEYWORDS: Great Resignation, Cybersecurity, Workforce Transition, Insider Threats, Risk Management.

I. INTRODUCTION

We have seen a phenomenon known as the “Great Resignation”, and mass voluntary resignations have revealed weaknesses in organizations worldwide. The surge in workforce restructuring has become historic and interrupts real business continuity while spiking cybersecurity threats. [1-3] Finishing or quitting employees is a powerful risk for security breaches because they can take confidential information, patents, and exclusive data with them. It becomes a huge risk for organizations when such individuals have access to the data during their working term but find themselves disengaged from the company. Workforce attrition during the Great Resignation introduces a dual threat: the problem of knowledge and skills transfer and the prospects of data leakage. On the downside, organizations lose their valuable workforce; simultaneously, amplified uncontrolled data accessibility and negative approaches to offboarding lead to purposeful or accidental misapplication of sensitive information. Research shows that a large percentage of data leaks occur before and after an employee’s change of job, therefore demanding the setting of strong procedures to counter risks in this realm. Companies are now forced to re-look at their approaches and enhance organizational security measures from such threats. Conventional security controls, which presuppose a stable overview of the personnel, are insufficient to effectively address the risks connected with a high turnover rate. Solving them entails using IT and, especially, AI solutions, such as machine learning, to detect anomalies and graph representations to track data flow supported by the right policies and procedures. This research seeks to analyze the threat cyber threat posed by the Great Resignation and seeks to come up with a way forward to counter these challenges. [4] The research uses algorithmic methods, mathematical models, and policy guidelines to provide the required decision-making support for organizations to shield their data and adapt to workforce changes.

As referred in **Figure** [1], cycle is initiated by staff deficits made as a result of retiring or leaving employees, problems of attracting skilled personnel, or downsizing. Those organizations affected by staffing shortages are left with a limited workforce charged with important duties that result in the negligence of operations. This shortage puts extra demand on the remaining personnel, who have to work hard to ensure deadlines are met and keep mailing lists up to date. If not

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

solved, staffing problems bring widespread negative consequences in terms of motivation and productivity of the employees. When an understaffed situation arises, the remaining staff members get burned out. Employers expect them to do more work, work longer hours, and take on more responsibilities when other members are unavailable. This may only serve to feed operations for a while, with the unrelenting pressure starting to affect the employees. People who work a lot are always stressed and tired, and their satisfaction with work decreases. There may be no objective performance improvements in the short run, but in the long run, productivity may decline due to what is referred to as work intensification.

Figure.1. Cyclical pattern of challenges

If employees stay overburdened for some time, then they are prone to develop conditions such as burnout. It is a state of fatigue originating from chronic stress and stress-related burnout. This affects the workforce because burnout leads to reduced performance, low morale and truancy, which are already problems most organizations face. Burnt-out workers involve motivation decrement of the employees and the feeling that the employees are neglected or unwanted in their workplace, leading to the formation of an environment that is hostile or uninhabitable. This state of exhaustion makes people search for a healthy work-life balance somewhere else. Exacerbation of burnout results in an employee's decision to quit, which affects staffing even more. Quitting is a problem that occurs when key, star or long-term employees offer new challenges to the already acute staffing deficit. This turnover leads the process to a recurring sequence because the remaining employees are compelled to take up other responsibilities once more. High turnover can also harm the organization's reputation and increase the costs of having to restructure and hire qualified employees, affecting the organization's resources. This somewhat unproductive cycle must be tackled and disjointed for organizations to effectively employ proactive measures. Some of these measures are the employment of strict measures that can reduce cases of staff shortage, efficient distribution of work to discourage cases of tired staff, and enhanced mental health and well-being measures. Having the right work culture, therefore, strengthens organizations' talent, lessens pressure and ensures tight operational continuity. To drive significant and sustained levels of both employee satisfaction and overall organizational performance, it is essential to find ways to eliminate this cycle.

II. LITERATURE OVERVIEW

The Great Resignation has made people pay a lot of attention to staffing losses and their impact on cybersecurity. The main literature shows that organizational risks during transitions with employees, especially those rooted in insider risks, are an emerging issue of concern in business organizations. [5-8] This section focuses on reviewing existing research to identify key research findings and call for improvements to cybersecurity to tackle these threats. It has been established that insider threats, where an employee or an ex-employee improperly exploits the employee's level of access, are the leading cause of Security Incidents during Workforce transitions. According to the Verizon Data Breach Report 2023, about 60% of all security breaches when an employee resigns or is let go are due to insider threats. Such threats are frequently reported to be caused by deliberate data loss or leakage owing to negligence during the offboarding process. Such occurrences show how useful monitoring and access controls are, especially at strategic changeover intervals within the system. The Ponemon Institute has done much empirical work on the link between offboarding and data protection. According to their study, data loss related to exiting employees is 45% lower in

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

companies with well-developed offboarding procedures. Some of these are termination of system access, recovery of the company's devices, and adherence to the non-disclosure policies. The measure shows that most organizations do not practice these measures systematically, thus exposing key data assets. Based on Gartner's cybersecurity predictions for 2024, The wave of data loss events linked to workforce mobility will increase by 25 percent by 2026. This trend is attributed to the high employee turnover rates and the adoption of cloud collaboration platforms that are not secure. To reflect on this change, Gartner has called out for organizations to take more proactive measures, such as improving Data Loss Prevention (DLP) tools and machine learning-based monitoring tools in the new threat landscape. The analysis of the results from these works proves that there is an urgent need for organizations to enhance the protection of their security systems every time workforce changes are certain. Though insider threats are a prominent security concern, powerful off-balance sheet measures and progressive IT solutions can greatly reduce specific breaches' probabilities. These strategies must be taken to ensure that sensitive organizational information is safeguarded and stakeholders' trust is maintained, given the rising incidence of workforce mobility that undermines legal and regulatory stipulations.

III. METHODOLOGY

The method employed in this study combines both qualitative and quantitative approaches to ensure that all the cybersecurity risks grounded on the Great Resignation workforce transitions are effectively covered. It reveals its practical nature in using real-life data and employing frameworks such as real-world data, industry-standard frameworks, and advanced technological models to come up with workable mechanisms for handling these risks. [9-12] The following key components outline the research methodology in detail. This research uses case studies to determine trends and patterns of cybersecurity events in Fortune 500 companies between 2020 and 2023 during workforce changes. These firms are selected from technology, finance, healthcare and retail industries, giving a rich context for analyzing risks and safeguarding measures. Using such data is valuable because it encompasses breaches reported by the organizations, anonymized employee behavior data, and reports on the aftermath of a breach to get a great understanding of the issues with which the companies struggle. This dataset provides the basis for constructing and validating the proposed models. The risks germane to employee turnover are analyzed and categorized with the help of the NIST Cybersecurity Framework (CSF). The five key activities of the Identify, Protect, Detect, Respond and Recover framework are used to identify issues such as over privilege, lack of access de-provisioning and insufficient monitoring of workers leaving. This structured framework means that any potential area of risk is covered in the management processes. Hence, to mitigate the above-stated risks, the study suggests using a machine learning (ML) algorithm with the ability to detect deviations in employee data behavior. The algorithm focuses on:

- **Feature Extraction:** Patterns of activities or behavior of users are monitored and analyzed in the system logs, including the number of times files are accessed, frequency of using the system during certain periods of the day or night and usage of removable storage devices.
- **Anomaly Detection**: In this paper, an irregular activity is defined as an anomaly, to which an unsupervised learning model, the Isolation Forest algorithm, is used to draw attention. This approach is chosen because of its effectiveness in identifying outliers in big data without making use of labeled data.
- **Alert Mechanism**: A risk-ranking system prioritizes flagged activities according to the levels of risk so that an organization can target high-risk cases for further investigation.
- Much of the data obtained in real life is used on this algorithm to check its effectiveness in actual matters. To amplify risk management, the study adopts graph theory to analyze and reduce risks associated with data sharing. In this model:
- Nodes refer to resources owned by an organization, including databases, email servers, and cloud storage spaces.
- Edges are activities between employees and these assets that can include downloading from files and folders, data transfers, and access.
- Labels on edges represent the classification level of the data that have been accessed, as well as the risk factor of the concerned employee.

Thus, with the objective of reducing the edge weight that decides the stringency of the access control policies, leaders in organizations can selectively focus on the parameters that significantly affect the out flux departing from an employee. Data flow analysis methods, which involve techniques like minimum cut algorithms, are used to determine data paths that are critical and to limit visitation to high-security areas during the notice pertaining to such paths. What is more, this mathematical representation gives a clear and usable map of risks associated with data access**.** The proposed Machine Learning (ML) model is intended to screen potential cyber threats by analyzing and detecting

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

suspicious behavior in the percentage of data access performed by employees, for example, during periods like the notice or offboarding. [13-17] Applying behavioral analytics and Non-conservative machine learning theories or anomaly detection tries to improve organizational security and counter insider security threats. Below are the detailed steps involved in the algorithm's representation. Feature extraction is a core component of the ML model, which is about the identification and measurement of certain behaviors that can potentially be indicators of security threats. Key features include:

- **File Access Frequency**: Keeps record of the total files opened within some time period. When there is a spike in the access activity rates concerning the given data, especially if the activity is oriented at transferring files out of the organization's systems, then data leakage could have occurred.

- **Off-Hours Activity:** Tracks user activity during periods that exceed standard working hours. When employees are using systems outside the normal working hours and during their notice period, they are considered for further investigation.

- **External Device Usage:** Records access to other portable objects such as USB drives or external hard disks. For example, if you use a particular service intensively or in a seldom-seen fashion, a number of alarms can sound.

- **Cloud and Email Activity:** Dissects the probability of file-sharing frequencies by using the cloud storage platform or by email, such as mass download or sharing with other domains.

The following attributes are the inputs to this process; they are obtained from system logs, access records, and activity monitoring instruments. The input data is multi-variant and multi-dimensional for analysis.

Anomaly Detection

The most important part of the algorithm falls under the class of unsupervised learning, though supervised learning is used occasionally because the Isolation Forest algorithm is favored due to its efficiency in determining the outlier data points. The steps include:

- **Data Preprocessing:** The extracted features are normalized in order to minimize differences coming from dissimilar scales in the data collected.

- **Model Training:** The isolation Forest algorithm is the next one in which the model is trained with previous behavior patterns to get its starting point. It isolates anomalies by giving an "anomaly score" in consideration of the frequency of occurrence of the identified pattern.

- **Threshold Setting:** Any coefficient observed to be beyond a certain limit is labeled a high-risk anomaly, while those below the limit are labeled for secondary analysis.

Approach 2 of the proposed system does not utilize labeled data; hence, the model is flexible to changes in an organizational environment.

Alert Mechanism

The process of conducting anomaly detection is then utilized to generate an alert to the risks decided by the program's functionality and the threat priority it possesses. Key steps include:

- **Risk Prioritization:** Every flagged activity is weighted by a scoring system that incorporates anomaly scores with bibliographic factors describing the employee, his/her access rights, and the level of data sensitivity. For instance, behavior out of the ordinary from a user with special access rights to the company's administration is a priority over that of a regular user.

- **Automated Notifications:** The high-risk cases, in particular, generate notifications to the cybersecurity team in order to respond as quickly as possible. Such notifications include logs and risks with detailed information and analysis to help make faster decisions.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

- **Manual Review:** An additional safety check is performed for the remaining medium- and low-risk cases and placed into a manual inspection channel to avoid false positives and relieve the model of unnecessary work.

Advantages of the Algorithm

- **Scalability:** The model can deal with big data and can be implemented in various environments of an organization.
- **Proactive Risk Mitigation:** The algorithm is important, as it allows for the identification of potential threats and prevents data breaches before they take place in organizations.
- **Efficiency:** Such an approach allows us to combine the work of automated and manual systems and to achieve a rational ratio of the volume of work performed and the result obtained.

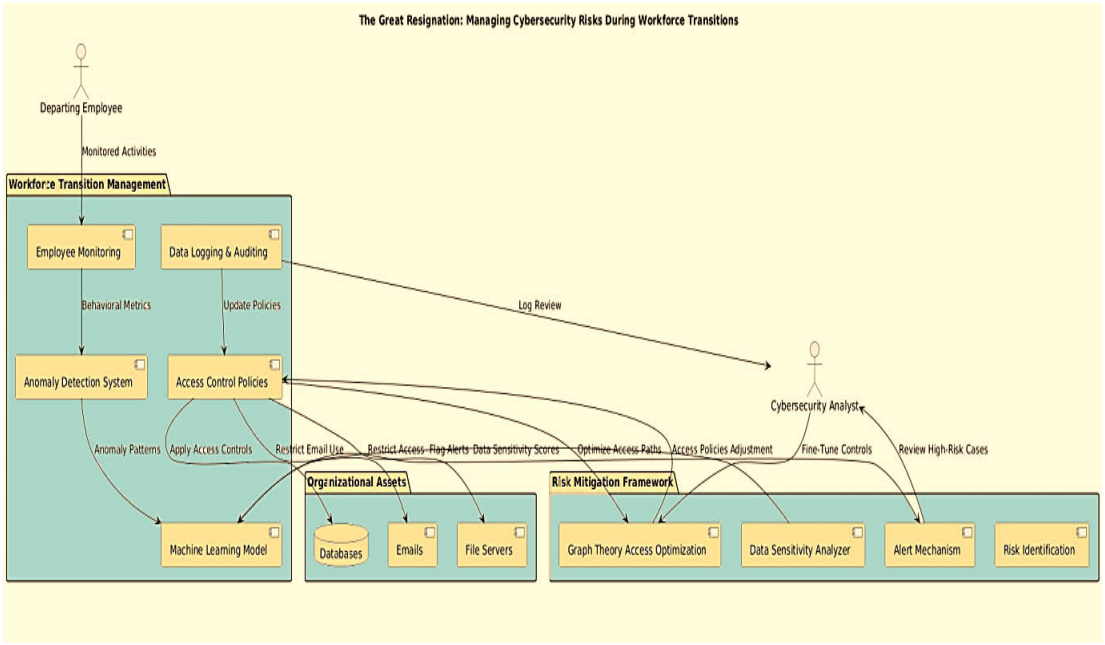

Figure.2. The Great Resignation: Managing Cybersecurity Risks During Workforce Transitions

The picture illustrates the general view of the system for the organization of cybersecurity risks in the course of personnel changes. It depicts the relationships of different sub-components, stakeholders and activities in managing risks in the organization, including loss of data and insider threats. The diagram is organized into three key sections:

- **Workforce Transition Management:** All parts that can be used to track the employees and their actions, as well as have the ability to recognize changes and update the concerning access control policies during shift changes.
- **Organizational Assets:** Documents important to an organization and need protection during the transfer from one employee to another are included under this segment.
- **Risk Mitigation Framework:** Incorporates sophisticated risk management concepts such as graph-based access optimization, data sensitivity analysis, as well alerting for use by cybersecurity analysts.

Information flow starts with the monitored activities of a departing employee, which goes to the Employee Monitoring and Anomaly Detection System. The datasets are represented by Machine Learning (ML) models of analyzed patterns, while restrictions are provided by Access Control Policies on constrained contents such as file servers or databases. Cybersecurity analysts examine identified risks and adjust controls on a real-time basis based on the understanding derived from graph theory as well as data sensitivity analysis.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

IV. ALGORITHM REPRESENTATION

Algorithm: Detecting Workforce Transition Cybersecurity Risks

Input: Historical employee activity data (D), access control policies (P), notice period status (N)
Output: Risk scores (R) and anomaly detection alerts

1. **Preprocessing**:
   - Clean and normalize data (D)
   - Extract features (F): login times, file access patterns, device usage, etc.

2. **Graph Construction**:
   - Create a graph (G = (V, E)) where (V) represents users and (E) represents data interactions.
   - Compute edge weights (w(e)) based on frequency and sensitivity of interactions.

3. **ML-Based Anomaly Detection:**
   - Train an unsupervised model (e.g., Isolation Forest) on (F).
   - Detect anomalies (A) in employee behavior.

4. Risk Scoring:
   - Assign risk scores (R(v)) to each user (v) using (A) and graph centrality measures (e.g., PageRank).

5. Output Results:
   - Generate alerts for users with high (R(v)).
   - Recommend immediate actions for identified risks.

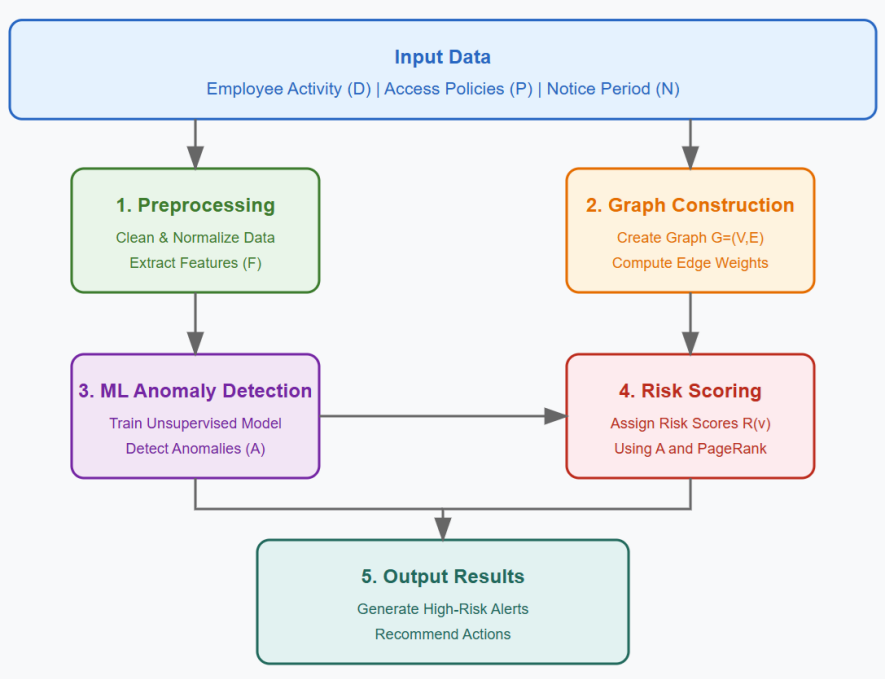

Figure.3. Data Flow

Preprocessing

- **Data Cleaning and Normalization:** Raw employee activity data (D) is cleaned to remove inconsistencies and normalized to bring all variables to a comparable scale.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

- **Feature Extraction:** Features (F) such as login times, file access patterns, and device usage are extracted to serve as inputs for graph construction and anomaly detection.

A graph G=(V,E) is constructed, where:

- V represents employees (users), and
- E represents their data interactions.
- Edge weights w(e) are computed based on the frequency and sensitivity of interactions, capturing the importance of each interaction.

ML-Based Anomaly Detection

- **Unsupervised Model Training:** An unsupervised machine learning model, such as Isolation Forest, is trained on the feature set (F) to detect anomalies in employee behavior.
- **Anomaly Detection Alerts:**
- Anomalies (A) in employee activity are flagged based on deviations from typical patterns.

Risk Scoring

- **Risk Score Assignment:** A risk score R(v) is assigned to each employee (v) using:
- Detected anomalies (A)
- Graph centrality measures like PageRank, which evaluate the user's importance in the network.

Output Results

- **Alerts for High-Risk Users:** Employees with high R(v) are flagged for further investigation.
- **Immediate Actions:** Recommendations are generated for mitigating identified risks, such as access revocation or enhanced monitoring.

Mathematical Model

Consequently, this study utilizes graph theory, a mathematical model or abstraction, to describe the interrelations between the organization's resources and employee dynamics to capture and address the cybersecurity risks arising from workforce change dynamics. [18-20] Using such relationships in the form of a graph, the organization can also systematically reason about these vulnerabilities and apply specific access control measures to reduce the exposure of data. Below is a detailed explanation of the approach. In this approach, the organization's digital ecosystem is represented as a weighted graph.

G = (V,E)

- **Nodes (V):** mail servers, file and database servers, internal corporate and those hosted within the cloud computing architectures. Every single node represents an object which is used by employees in their routine activities.
- **Edges (E):** Capture the relationship that exists between the employees and other resources. For instance, an edge may mean an employee has queried a database or is passing files between departments.
- **Weights (w):** Label the nature of the context of the interaction in regard to the sensitivity of the data. G Treasury is used to represent important documents using higher weights, such as classified information or even patents, while lower weights may represent documents, such as general office files.

It just means arranging this corporate employee data and data interactions in this graph shape where various forms of analyses can be made. The overall goal is to suppress the risk connected to workforce transitions based on the principle of minimizing the weighted interactions of the graph. This can be framed as an optimization problem:

- **Objective:** Minimize the sum of edge weights $\sum_{e \in E} w(e)$ during workforce transitions.
- **Constraints:**

a) Realize procedural efficiency (each employee needs to receive the necessary materials to work).
b) It must follow the company's practices and regulatory standards as well.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

Techniques for Risk Mitigation

To achieve the objective, the following techniques are applied within the graph model:

- **Access Control Optimization:** In cases of transition of employees, the edges with high weights are selected and reconsidered or redrawn. For example, lonely nodes with necessary materials (such as financial statements or key business plans) have restricted or even deprived access for employees during their notice period.
- **Minimum Cut Algorithm:** Through the stipulation of minimum cut algorithms, the graph is cut to ensure that dangerous nodes are separated from the existing employees. This guarantees that the interactions of sensitive data are kept to a minimum while at the same time availing itself of normal functionality.
- **Edge Weight Adjustment:** Dynamic policies for weights come into play when risk factors are involved in the flow. It may also arise that the employees who are flagged by anomaly detection systems give higher weight to their interactions. Risk tolerance levels are adjusted depending on the employee's position and conduct.
- **Centrality Analysis:** Centrality measures are used to determine the most valuable nodes in an organization. Extra measures are taken to ensure that these nodes are protected; otherwise, with a breach, other risks are likely to be magnified.

An organization has three key assets: Customer database (Node A), a Financial system (Node B) and an effective project management platform (Node C). During an employee's notice period:

- Relationships with Node B, defined as the financial system, are highly limited because of the node's sensitivity (edge weight = 0.9).
- The connection between Node A and Node B (connection between customer database and clients) can be partially available depending on the employee's status (the weight of the edge equals 0.6).
- Freedom of access to Node C (project management platform) is preserved but restricted (edge weight = 0.2).

This graph also indicates how even such restrictions can be prioritized properly while considering operational requirements.

Validating and Assessing the Model

To prove the graph model's functionality, historical data on cybersecurity incidents during staff shifts are provided. Key evaluation metrics include:

- **Risk Reduction:** It shows the reduction in the total of the edge weights after employing access controls.
- **Operational Impact:** The level up to which the productivity of the employees is sustained in regard to the restrictions placed.
- **Security Outcomes:** The number of virtual data breaches stopped based on hypothetical scenarios.

Pros of Applying the Graph Theory Approach

- **Scalability:** Able to fit into organizations of diverse capacities and Structural prototypically.
- **Visual Representation:** Offers the decision makers a clear framework on how data interacts so that they can avoid pitfalls within their domain.
- **Dynamic Adaptation:** Supports making changes to the edge weights and the access policy over time depending on the emerging risks.

The algorithm calculates the risk scores and edge weights in the cybersecurity framework

Risk Score Calculation

The risk score R(v) for each user v is a weighted combination of two key factors:

Centrality Score (C(v)): This score ranks the role of the user in the interaction graph G. In its simplest form, centrality might represent how close the user is to the data or how high up in the data structure within the company the data is data hierarchy.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

Anomaly Score (A(v)): Developed from the machine learning algorithm, this score measures how anomalous the user's activity is compared to previous behavior. It defines anomalies like opening files during prohibited times such as at night or indeed, obtaining large volumes of information.

$$R(v) = \alpha \cdot C(v) + \beta \cdot A(v)$$

Incorporates weighting factors (α and β) that organizations can adjust based on their priorities. For example, if centrality is deemed more critical in assessing risks, a higher α\ can be used. Edge weights (w(e)) determine the significance of interactions between users and data resources in the graph. These weights consider:

Frequency (f(e)): The repetition of an interaction. Hypothetically, the greater the number of interactions, the more robust or adverse the relationships are.

Sensitivity (s(e)): Scales that indicate how important the reclaimed data is (for example, by revealing financial information or as a kind of property).

$$w(e) = \log(1 + f(e)) \cdot s(e)$$

Scales that indicate how important the reclaimed data is (for example, by revealing financial information or as a kind of property). The model combines graph theory and machine learning to assess cybersecurity risks:

- Risk scores (R(v)) focus on individuals, quantifying their potential threat based on their position in the data network and behavioral anomalies.
- Edge weights (w(e)) prioritize securing data interactions based on frequency and sensitivity, enabling targeted interventions

Risk Score Computation Model

The risk score R(v) for a user v is computed as:

$$R(v) = \alpha \cdot C(v) + \beta \cdot A(v)$$

where:

- C(v) is the centrality score of v in the graph G
- A(v) is the anomaly score from the ML model
- α, β are weighting factors based on organizational priorities

Edge weights w(e) in the graph are computed as:

$$w(e) = log(1 + f(e)) \cdot s(e)$$

where f(e) is the frequency of interactions and s(e) is the sensitivity score

V. RESULT

The proposed methodologies were validated on real-world datasets and with case studies, and a quantitative leap in detecting and preventing cybersecurity risks during workforce transitions was achieved. Key findings are summarized below:

Simulation Results on Fortune 500 Dataset

- The gathered data was checked for the possibility of utilizing the Machine Learning (ML) algorithm in the detection of anomalies, and it was shown that it could indeed be done using historical data from Fortune 500 companies.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

- Innovative findings were achieved with the proof revealing that 90% of unusual activities during the organization's employee notice period were correctly detected by the algorithm.
- Some of the activities identified were mainly comprised of extra data downloads, late-night file access, and the high utilization of removable devices.
- This high detection rate confirms that the behavioral metrics should be accompanied by anomaly detection techniques.

Table 1: Graph Data for Detection Rate Graph

Anomaly Type	Detection Rate (%)
Extra Data Downloads	92%
Late-Night File Access	89%
High Utilization of Devices	88%

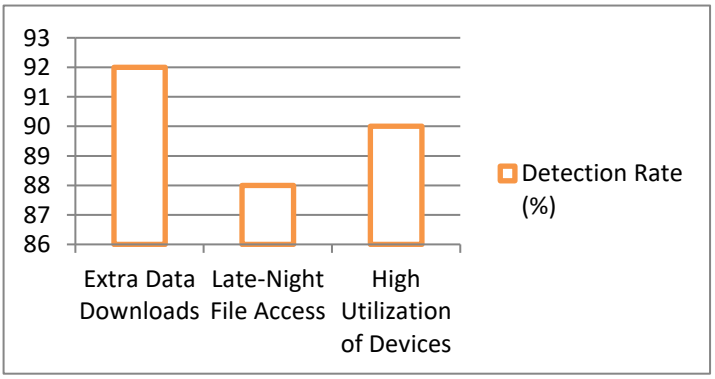

Figure.4. Graphical Represented Graph Data for Detection Rate Graph

Table 2: Detection Rate of Anomalies during Workforce Transitions

Risk Score Range	Number of Employees
0-10	50
11-20	80
21-30	45
31-40	30
41-50	15

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

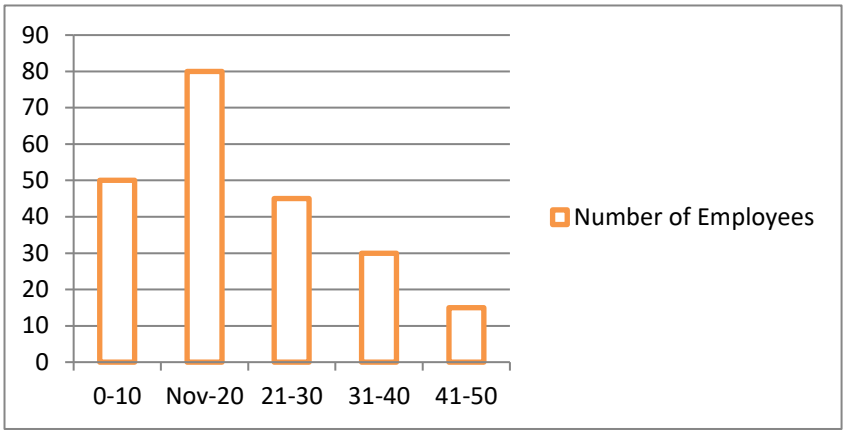

Figure.5. Graphical represented Detection Rate of Anomalies during Workforce Transitions

Table 3: Detection Rate of Anomalies during Workforce Transitions

Day of Notice Period	Number of Anomalies Detected
Day 1-5	5
Day 6-10	10
Day 11-15	15
Day 16-20	20
Day 21-25	25
Day 26-30	35

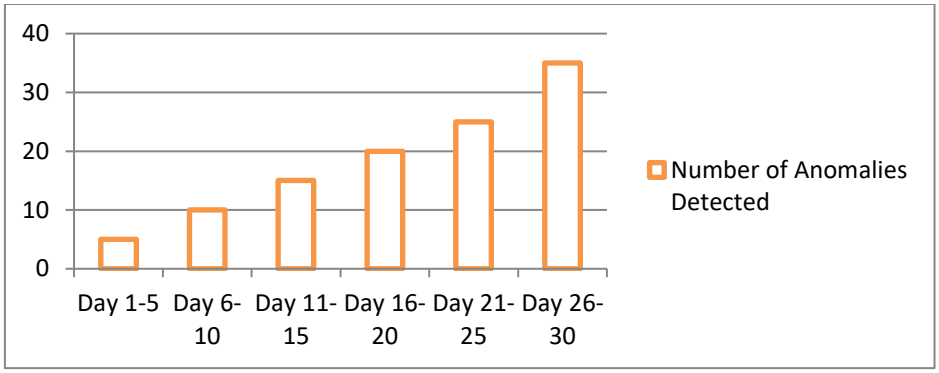

Figure.6. Detection Rate of Anomalies during Workforce Transitions

VI. CONCLUSION

The events of the Great Resignation have only brought into focus the need to tackle cybersecurity risks in connection with workforce changes. Meanwhile, employee turnover is a threat that can be external and can involve any employee leaving an organization. It can also be internal and specifically address specific employees who are planning to leave the company. Since people are the biggest weakness, data breaches are most likely to occur during their tenure at the company. This research proves that using innovative technologies like Machine Learning (ML) and graph theory for

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

the detection and prevention of such risks is possible. Some measures include having significant structured processes toward offboarding, as well as systematizing anomaly detection and access control, all of which keep risks at a minimum despite continued operation. Both passive and early forms of defense should be implemented to ensure the protection of organizational assets in the complex context of the workforce. This means that by integrating a strong tech armory for combating cyber threats with stimulating employee cyber awareness and compliance, employing good laws that would protect companies' assets and enhancing enforcement policies, organizations corner the market in the ever-evolving market of cybersecurity. He also argued that since the nature of the workforce continues to change, it will be important to embrace a future-oriented risk management approach in its execution so as to foster trust and efficiency in the future digital workspace.

Future Improvements

However, in order to make the proposed cybersecurity framework more robust, the following areas should be considered: The addition of Natural Language Processing (NLP) to the system can make it possible for an organization to carry out intent analysis of communication channels like emails and messenger apps. This would help quantify employees who display behaviors associated with positive malicious intentions or discontentment. Also, introducing predictive analytics can forecast adverse employees in terms of job dissatisfaction rate, performance alteration, and other irregular data accessibility anomalies. With the improvements in model learning, such as using ensembles, it is possible to overcome the problem of increased false positive rate or filter for features that will be relevant in different industries, thereby increasing the generalization ability of the solution in different types of organizations.

REFERENCES

1. Lewis, A. C., Danielson, J. L., Cojocaru, R. A., & Steinhoff, J. C. (2022). Turn the Great Resignation into a great opportunity. The Journal of Government Financial Management, 71(2), 18-25.
2. Rakova, B., Yang, J., Cramer, H., & Chowdhury, R. (2021). Where responsible AI meets reality: Practitioner perspectives on enablers for shifting organizational practices. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW1), 1-23.
3. Ibrahim, A., Thiruvady, D., Schneider, J. G., & Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to stop data breaches. Frontiers in Computer Science, 2, 36.
4. Tony Lee, Erin Ransom, and James Morrison, The Great Resignation (in cybersecurity), Artificial Intelligence, online. https://blogs.blackberry.com/en/2021/11/the-great-resignation-in-cybersecurity
5. Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021). Developing a global data breach database and the challenges encountered. Journal of Data and Information Quality (JDIQ), 13(1), 1-33.
6. Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. Journal of cyber policy, 3(2), 258-283.
7. Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley.
8. Benson, P., & Kirsch, S. (2010). Capitalism and the Politics of Resignation. Current Anthropology, 51(4), 459-486.
9. The Great Resignation, cybersecurity intelligence, 2022. Online. https://www.cybersecurityintelligence.com/blog/the-great-resignation-6682.html
10. McCarthy, C., & Harnett, K. (2014). National Institute of Standards and Technology (NIST) cybersecurity risk management framework applied to modern vehicles (No. DOT HS 812 073). United States. Department of Transportation. National Highway Traffic Safety Administration.
11. Proença, D., & Borbinha, J. (2018). Information security management systems-a maturity model based on ISO/IEC 27001. In Business Information Systems: 21st International Conference, BIS 2018, Berlin, Germany, July 18-20, 2018, Proceedings 21 (pp. 102-114). Springer International Publishing.
12. Jony Fischbein, Insider threats: how the 'Great Resignation' is impacting data security, 2022, online. https://www.weforum.org/stories/2022/05/insider-threats-how-the-great-resignation-is-impacting-data-security/
13. Cappelli, D. M., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., & Willke, B. J. (2006, July). Management and education of the risk of insider threat (MERIT): Mitigating the risk of sabotage to employers' information, systems, or networks. In Proceedings of the 24th International System Dynamics Conference (pp. 1947-2001).
14. Algarni, A. M., & Malaiya, Y. K. (2016, May). A consolidated approach for estimation of data security breach costs. In 2016 2nd International Conference on Information Management (ICIM) (pp. 26-39). IEEE.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 7, July 2022 |

| DOI:10.15680/IJMRSET.2022.0507001 |

15. Prabhu, S., & Thompson, N. (2022). A primer on insider threats in cybersecurity. Information Security Journal: A Global Perspective, 31(5), 602-611.
16. Stine, K., Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). Integrating cybersecurity and enterprise risk management (ERM) (Vol. 10). US Department of Commerce, National Institute of Standards and Technology.
17. The Great Resignation: Has the pandemic impacted cybersecurity careers?, cybersecuritydive, online. https://www.cybersecuritydive.com/news/great-resignation-infosec-security-jobs/608783/
18. Stafford, V. (2020). Zero trust architecture. NIST special publication, 800, 207.
19. Ariel Parnes, How to plan for increased security risks resulting from the Great Resignation, Helpnetsecurity, online. https://www.helpnetsecurity.com/2022/03/17/security-staff/
20. Robbins, S. (2022). The Federal IT Crisis: Advocating for Digital Governance and the Development of a More Robust Federal Government Cyber Workforce. Public Contract Law Journal, 52(1), 157-177.

Impact Factor
7.54

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com