KARYA ILHAM PUBLISHING
CONNECTING MINDS, BRIDGING IDEAS, INSPIRING READERS

Journal of Advanced Research in Business and Management Studies

Journal homepage:
https://karyailham.com.my/index.php/arbms/index
ISSN: 2462-1935

Big Data-Driven Information Security Behavioural Profiling for Organisational Resilience

Najwa Hayaati Mohd Alwi[1,2,*], Hanifah Abdul Hamid[1,2], A H Azni[1,2], Farida Ridzuan[1,2], Odai Enaizan[3]

[1] Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, Malaysia
[2] Cybersecurity and Systems Research Unit, Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, Malaysia
[3] Department of Management Information Systems, College of Haql, University of Tabuk, Tabuk 71491, Saudi Arabia

ARTICLE INFO

Article history:
Received 7 July 2025
Received in revised form 22 August
Accepted 28 August 2025
Available online 5 September 2025

Keywords:
Users behaviour profiling; information security; big data; organisational resilience

ABSTRACT

As cyber threats become more common, it is imperative to comprehend the behavioural patterns that contribute to security risks to bolster organisational resilience. This study aims to discover particular actions before security incidents in organisations by utilising big data analytics on survey responses to reveal these patterns. The main goal is to identify employee behaviours that are security vulnerabilities in order to gain practical insight for proactive risk management. A survey is conducted to collect data from various departments within the selected organisation. The survey gathered information regarding individuals' daily routines, compliance with security protocols, responses to security training, and past experiences with security breaches. The gathered information was analysed to find patterns and trends in behaviour associated with increased security risks. The study findings emphasise the importance of monitoring these behavioural indicators in order to enhance organisational resilience. Organisations can successfully reduce risks by understanding and dealing with these basic behaviours, implementing targeted interventions, improving security training programmes, and refining policies. This study provides valuable information on key indicators of employee behaviour that can be used to proactively tackle security risks, making a significant contribution to cybersecurity and the overall resilience of the organisation. The results derived from this study offer practical recommendations for organisations to enhance their defence against cyber threats by implementing informed behavioural monitoring and management.

1. Introduction

Organisations today face an ever-evolving landscape of cyber threats, ranging from malware and data breaches to sophisticated phishing attacks. Due to the dependency of organisations on information technology, protecting sensitive data and systems has become a critical priority. In 2023,

* *Corresponding author.*
E-mail address: najwa@usim.edu.my

https://doi.org/10.37934/arbms.40.1.100110

it was reported that the loss due to cyber-attacks globally amounted to approximately $8 trillion [1], underscoring the significant financial and operational impact these threats pose to businesses of all sizes. Effective proactive risk management strategies are crucial for organisations to maintain operational resilience and safeguard their assets in this challenging environment. One of the vulnerabilities that cybercriminals can exploit is the human [2]. In organisations, employees' naive and unintentional behaviors, such as falling for social engineering tactics or using weak passwords, are frequently cited as the primary cause of security breaches [3,4]. Therefore, understanding employee behavior and developing strategies to mitigate these risks is crucial.

`

1.1 Profiling Employee's Behaviour

Profiling employees' behavior and leveraging data-driven insights can enhance information security and build organisational resilience [5,6]. Employee behavior and awareness play a vital role in organisational information security. Recent research highlights on human mistakes such as clicking on malicious links, sharing login credentials, and leaving devices unattended are common vulnerabilities cybercriminals can exploit [4]. Therefore, understanding employee security behaviors and actions that occur before security incidents in organisations is crucial for developing effective risk mitigation strategies. To maintain organisational resilience, it is essential to develop proactive risk management strategies beyond traditional perimeter-based security measures. One promising approach is using big data analytics to profile employee behavior and identify potential security risks [7].

The rise of big data and advanced analytics has transformed the field of cybersecurity, enabling organisations to gather and analyse vast amounts of data from various sources, including network traffic, user activities, and security logs [4]. By leveraging these data-driven insights, organisations can better understand employee behaviors, detect anomalies, and implement targeted interventions to mitigate security risks [8]. Profiling user's activities with data analytic techniques may give insights into building effective organisational control.

1.2 Importance of Understanding Employee Behavior

Employees play a critical role in an organisation's overall security posture. Research has shown that human errors and negligence are among the leading causes of security breaches in organisations [9,10]. Individuals' daily routines, compliance with security protocols, responses to security training, and past experiences with security breaches can all impact an organisation's vulnerability to cyber threats [11,12].

1.2.1 Daily routines and security risks

Understanding employees' daily routines is essential for identifying behavioral anomalies that could signal security risks. Recent research highlights deviations from regular work patterns, such as irregular login times or unusual access to sensitive data, can indicate potential insider threats. These anomalies can be detected through continuous monitoring and analysing user activity logs using big data analytics.

1.2.2 Compliance with security protocols

Employee adherence to security protocols is critical for maintaining organisational security. D'Arcy and Herath [1] emphasise that non-compliance often results from perceived inconvenience or lack of awareness about the importance of security measures. Regularly updated training and clear communication about the significance of these protocols can improve compliance rates. For instance, enforcing frequent password changes and using multi-factor authentication are vital areas where compliance must be monitored and enforced.

1.2.3 Responses to security training

The effectiveness of security training programs plays a pivotal role in equipping employees to recognise and respond to security threats. A study by Ifinedo [13] demonstrates that engaging and interactive training sessions significantly enhance employees' ability to detect phishing attempts and other security threats. The study also indicates that continuous training and periodic evaluations ensure that employees effectively retain and apply their knowledge.

1.2.4 Past experiences with security breaches

Analysing past security incidents offers valuable insights into potential vulnerabilities and effective mitigation strategies. Recent findings suggest that understanding the circumstances and responses to previous breaches can help organisations develop more robust security policies [14]. Employee involvement in these incidents can reveal gaps in current security measures and highlight the need for improved training and protocols.

1.3 Gaps in Existing Research

Prior studies in information security have concentrated on comprehending individual user behaviour by utilising established psychological and behavioural theories such as the Theory of Planned Behaviour (TPB), Theory of Reasoned Action (TRA), Protection Motivation Theory (PMT), Technology Acceptance Model (TAM), Social Cognitive Theory (SCT), General Deterrence Theory (GDT) and the Health Belief Model (HBM). The primary focus of these researches has been to assess and confirm these ideas by investigating how various elements, such as attitudes, intents, perceived threats, and self-efficacy, impact an individual's inclination to choose safe behaviours. Although these theoretical models have offered valuable insights into the psychological foundations of information security behaviour, they often prioritise forecasting behavioural intentions rather than watching and analysing actual behaviours in a practical organisational setting. Behavioural intentions, however suggestive, do not always result in immediate action. The disparity between workers' intentions and actions regarding information security may be substantial, impacted by several contextual, environmental, and situational elements that are not usually accounted for in research focused on intentions.

In addition, existing research on behavioral profiling in information security has primarily focused on individual user behavior, with limited attention paid to the broader organisational context and the role of employee behavior in enhancing organisational resilience [15,16].

This research aims to fill this void by redirecting attention from behavioural goals to tangible behaviours. This study seeks to experimentally examine the actual behaviour of workers concerning the elements found in the literature instead of relying exclusively on theoretical conceptions to

predict their behaviour. This research utilizes big data-driven behavioural profiling to analyse the activities of employees in a real-world organisational environment. The goal is to get a more precise and practical knowledge of security behaviors.

By focussing on real-life actions, a more detailed examination may be conducted to understand how workers engage with security procedures and regulations, how they react to cyber threats in real-world situations, and how these behaviours impact the organization's ability to withstand challenges. This technique also allows for the detection of behavioural patterns and trends that may not be apparent when just considering intentions, providing more comprehensive insights into the practical dynamics of information security inside an organisation.

This paper elaborates on a survey with the following:

1. to identify daily routines. This is to understand typical behaviors and routines of employees to detect anomalies.
2. to assess compliance with security protocols. This is to determine adherence to security policies and identify gaps.
3. to evaluate responses to security training. This is to gauge training programs' effectiveness and identify areas for improvement.
4. to analyse past experiences with security breaches. This objective is to learn from previous incidents to prevent future occurrences.

2. Methodology

To gather the necessary data for this study, the researchers distributed a survey across multiple departments within the selected organisation, seeking to gain insights into employees' daily routines, adherence to security protocols, responses to security training, and any past experiences with security breaches [4,9,15].

2.1 Data Collection

Survey instruments were developed by adopting and modifying previous studies that had explored the relationship between human behavior and cybersecurity vulnerabilities [17]. Questionnaires were distributed online via email and WhatsApp to ensure participation from diverse employees across the organisation, capturing perspectives from various departments and hierarchical levels. Ninety-one valid responses were gathered after five days of questionnaires were distributed. The data collected will be analysed as the initial result of the study.

2.2 Data Analysis

Data collected is analyzed using three different techniques. Descriptive analytics is employed to summarize survey responses, allowing for the identification of common behaviors and compliance levels. Regression analysis is used to estimate the effect of some explanatory variables on the dependent variable. Additionally, cluster analysis groups similar responses to uncover common characteristics of high-risk behaviors.

3. Results

This section discusses the results obtained from the survey conducted. There are 91 respondents, 70% female and 30% male. 59% are academicians, 32% are administrative staff, and 9% are supporting staff. Figure 1 depicts the age of the respondents ranging from 21-59 years old.

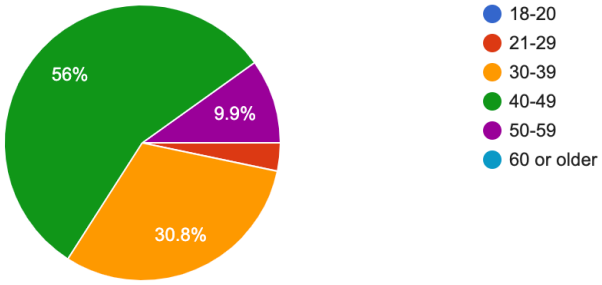

Fig. 1. Respondents age

3.1 Daily Routines

The respondents explain their daily routines, which include the typical workday schedule. All of them are using computers and the Internet for their daily job. Usually, they will log into the organisation's Wi-Fi to connect to the internet. When asked about login and logout behavior, 40% strongly agreed, and 30% agreed that they log in every time using their computer. At the same time, 50% indicated that they do not log out during break time. About 45% indicated that they always log out before closing the computer. The study also found that less than 40% of employees use the User Login Lifetime and the inactive logout Timer as the default settings while using the computer. The result shows in Figure 2 that these routines are prone to vulnerability and threats.

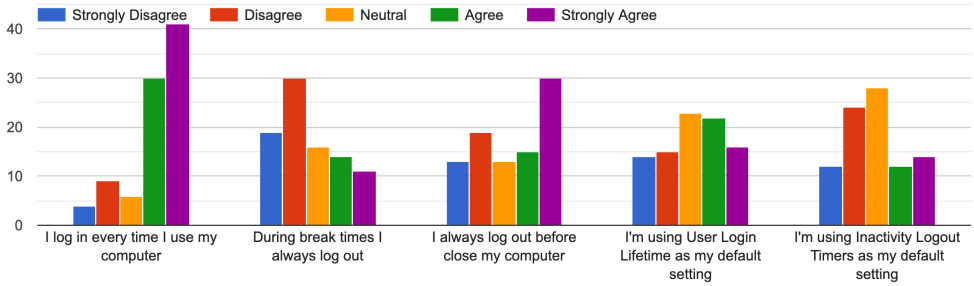

Fig. 2. Employee login and logout behavior

Irregular hours can be a sign of unauthorised access or potential security threats. Therefore, we ask how frequently they work outside regular office hours. As depicted in Figure 3, 58.9% choose to agree and strongly agree that they frequently work outside of regular office hours, while 23.3% choose neutral. Figure 3 is the detailed result of employee frequency accessing the company's network remotely. Remote access patterns can reveal potential vulnerabilities, especially if unsecured networks are used.

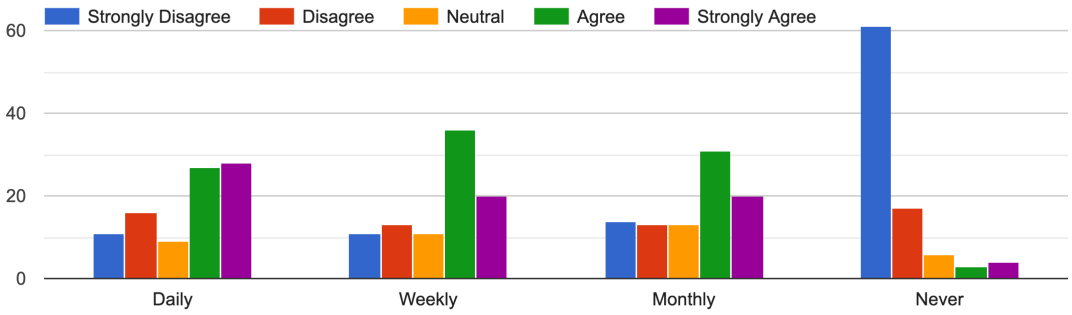

Fig. 3. Employee frequency access the company's network remotely (Daily/Weekly/Monthly/Never)

3.2 Compliance with Security Protocols

Questions were asked to assess how well employees follow security protocols and identify areas of non-compliance. Figure 4 indicated that 83.5% of the majority changed their passwords only when prompted. Figure 5 shows that 83.6% use MFA to access company resources. 93% of respondents claimed they never bypassed security protocols to complete a task.

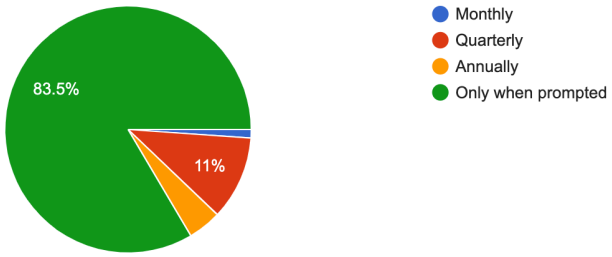

Fig. 4. Password changes

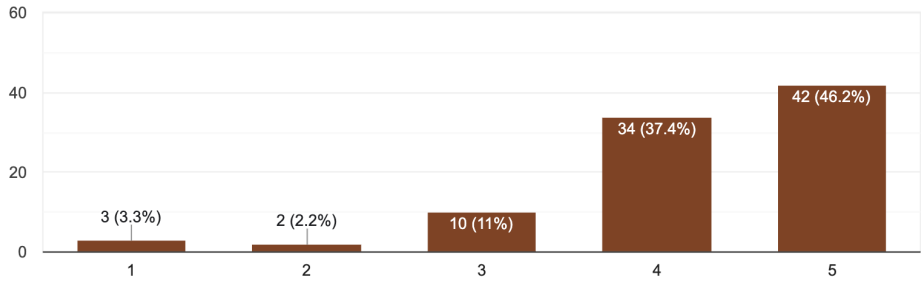

Fig. 5. Multi-Factor Authentication (MFA) usage for accessing company resources

3.3 Responses to Security Training

Questions were asked to gauge training programs' effectiveness and identify areas for improvement. Figure 6 indicated that 25.6% had attended training sessions in the past year. In Figure 7, 40% chose neutral when asked about the usefulness of the training attended. They also show confidence in recognising phishing attempts and other security threats, as in Figure 8.

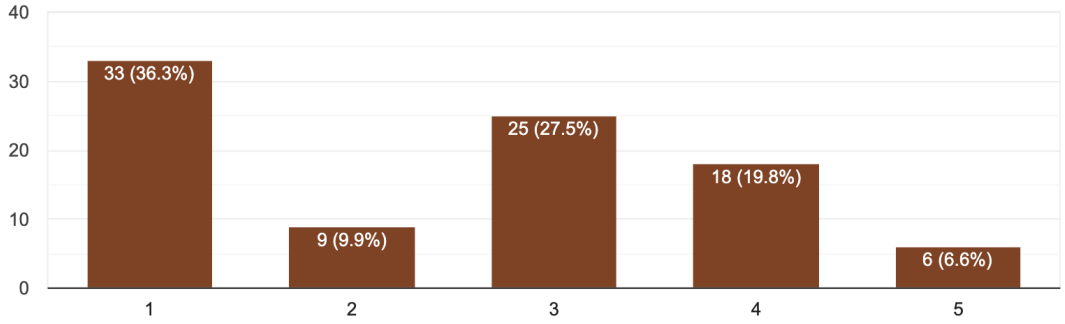

Fig. 6. Security training sessions attended in the past year

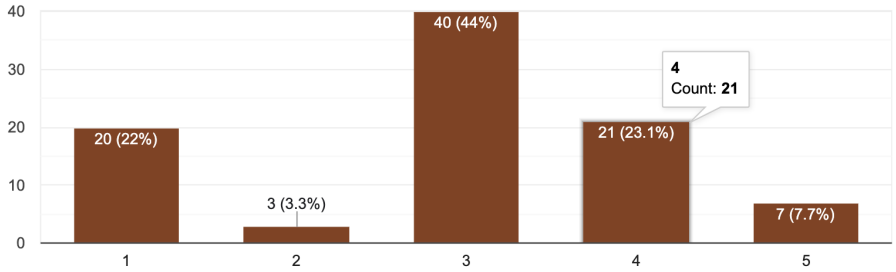

Fig. 7. Usefulness of the training attended

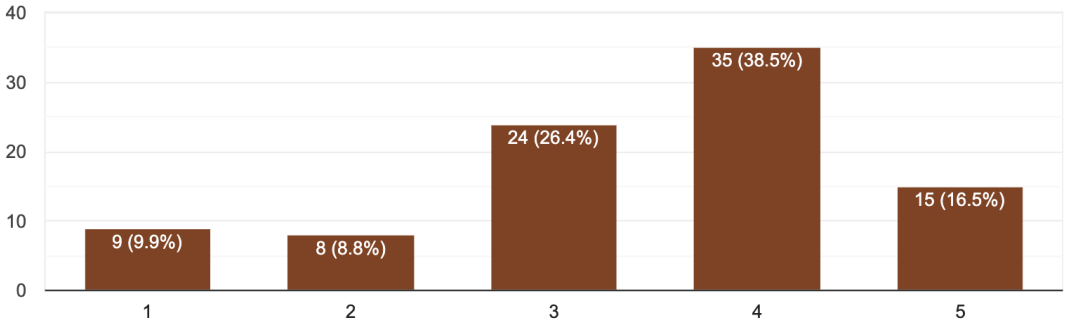

Fig. 8. Confident in the ability to recognise phishing attempts and other security threats

In addition to the descriptive analysis results, we performed regression analysis using Matlab for this section. The outcome revealed a discrepancy between the anticipated comprehension and the actual comprehension. Figure 9 illustrates the anticipated comprehension. According to Figure 10, the respondents tend to overestimate themselves, as some need more understanding or participation in the training. The control mechanism may have been implemented to address the issue of phishing.

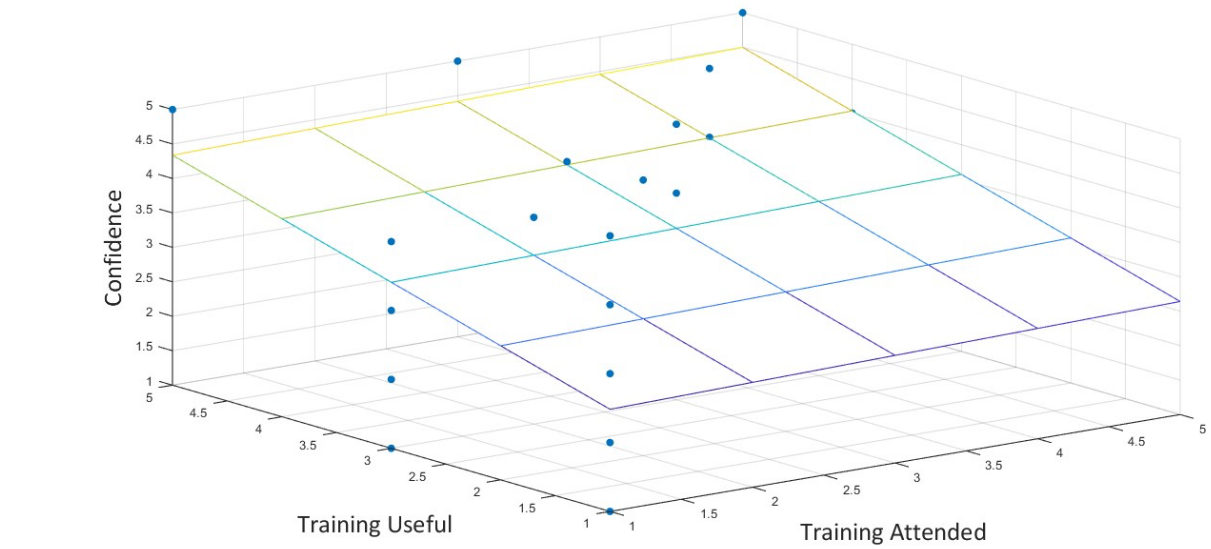

Fig. 9. 3D Scatter plot with regression plane

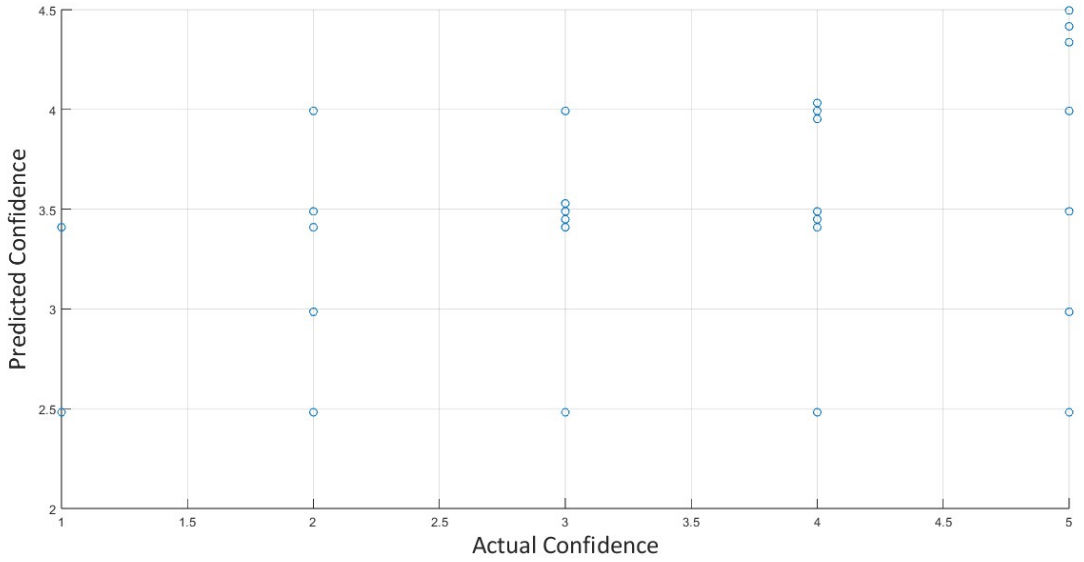

Fig. 10. Actual vs predicted confidence

While respondents may receive external information about phishing knowledge, organisations must offer comprehensive training to provide more in-depth and detailed knowledge.

3.4 Past Experiences with Security Breaches

To gain insights from previous occurrences and comprehend the firsthand encounters of employees with security breaches, they were queried about their involvement in any security breach or incident that took place at their workplace. The purpose of this is to identify employees who have firsthand experience dealing with security incidents. The survey findings revealed that a mere 8%

acknowledged their involvement in a security breach or incident at their workplace. This encompasses various cyber-attacks, such as email phishing, hacking through the Telegram messaging platform, and unauthorised access to computer systems. Additionally, they expressed comprehension of the organisational reaction to incidents and the efficacy of implemented modifications. It was mentioned that the organisation implemented Multi-Factor Authentication (MFA) and distributed security awareness posters.

A cluster analysis is conducted to understand the situation further, and the result is depicted in Figure 11. The clusters' colors indicate different categories of employee behavior, which are determined by factors such as individuals' daily routines, adherence to security protocols, reactions to security training, and previous encounters with security breaches. The centroid, also known as the mean value, is symbolised by the triangle. The Response to Security Training cluster revealed that the low positive habit score of user training awareness indicates a low level of security awareness in that area, with an average security awareness score of 4. However, the impact on security awareness remains significant despite the lower frequency of security breaches in past experiences, as indicated by the habit score. Past experiences with security breaches are more effective than security training awareness in providing protection.

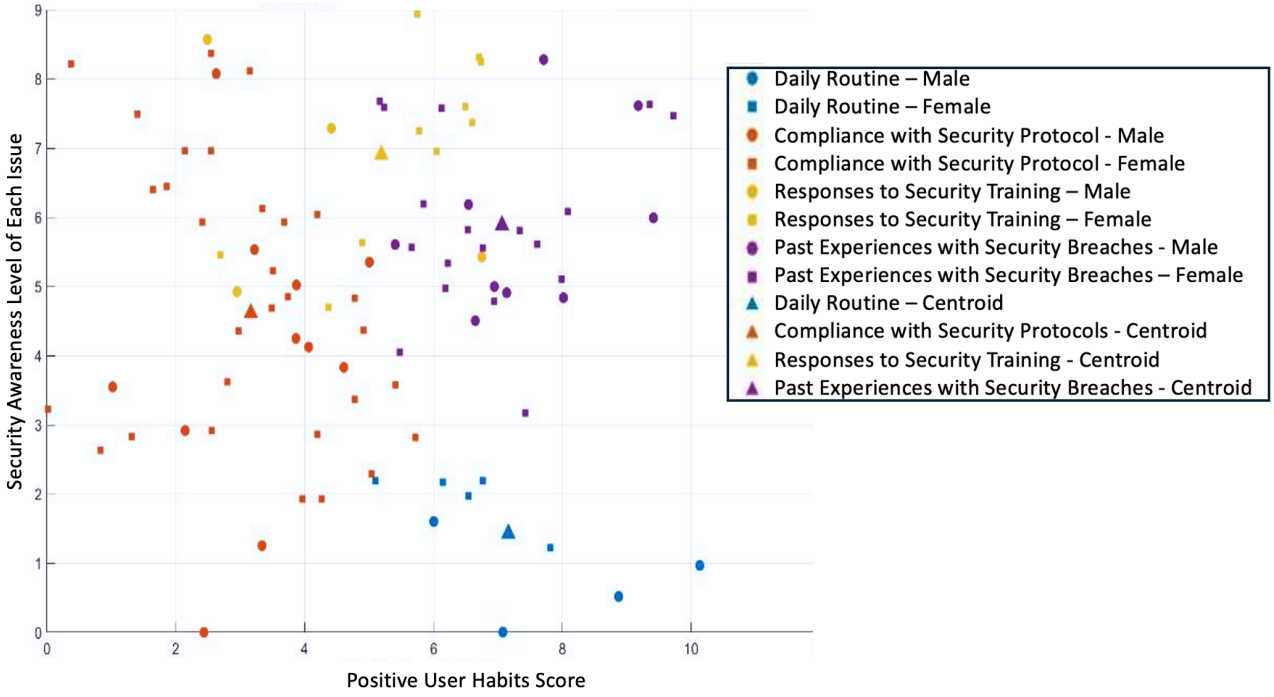

Fig. 11 Clustered scatterplot of intelligence data

The study has yielded several insights, including primary behavioral indicators that strongly correlate with security breaches, such as deviating from regular work hours or circumventing security protocols. It also identifies training deficiencies based on employee feedback and confidence levels, highlighting areas where security training can be improved. Additionally, it proposes revisions to security policies to rectify identified vulnerabilities and improve overall adherence to regulations.

Recommendations include enforcing specific training and policy updates to tackle behaviors that pose a high risk, implementing continuous monitoring to track and address significant behavioral indicators, and creating extensive training programs customized to target the specific requirements

and deficiencies identified in the survey. A recent study on behavior profiling suggests that organisations can shape employee security behavior by implementing comprehensive security education, training, and awareness programs targeting the human aspect of information security. The references cited are [7,18-22]. It is crucial to comprehend employees' conduct while working in an organisation.

4. Conclusions

This study underscores the critical importance of closely monitoring behavioral indicators to enhance organizational resilience. By understanding and addressing these fundamental behaviors, organizations can effectively mitigate risks through targeted interventions, improved security training programs, and refined policies. The findings provide practical insights into key employee behavior indicators that can proactively address security risks, making a substantial contribution to cybersecurity and enhancing the overall resilience of the organization. The primary limitation of the current study is the relatively small sample size of only 91 respondents. While this sample has provided some insights, a larger sample size could significantly enhance the reliability and generalizability of the findings. Additionally, the study was conducted using quantitative methods, which may limit the depth of understanding specific behavioral dynamics. To address these limitations and deepen the insights of this research, future studies should consider incorporating qualitative data that can provide richer, more contextual understandings of behavioral indicators. Increasing the number of respondents will also be a priority to ensure a broader representation and enhance the generalizability of the findings. This combined approach will aim to provide a more comprehensive view of the behaviors that influence organizational cybersecurity resilience.

Acknowledgement
This research was funded by a grant from Universiti Sains Islam Malaysia (**PPPI/USIM/FST/USIM/111423)**

References
[1] D'Arcy, John, Idris Adjerid, Corey M. Angst, and Ante Glavas. "Too good to be true: Firm social performance and the risk of data breach." *Information Systems Research* 31, no. 4 (2020): 1200-1223 https://doi.org/10.1287/isre.2020.0939

[2] Ab Halim, Azni Haslizan, Farida Ridzuan, Nur Hafiza Zakaria, Abdul Alif Zakaria, Najwa Hayaati Mohd Alwi, Sakinah Ali Pitchay, Ismail Az-Zuhar, and Ahmed A. AlSabhany. "SAKTI©: Secured Chatting Tool through Forward Secrecy." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 49, no. 1 (2025): 54-62 https://doi.org/10.37934/araset.49.1.5462

[3] Parsons, Kathryn, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, and Tara Zwaans. "The human aspects of information security questionnaire (HAIS-Q): two further validation studies." *Computers & Security* 66 (2017): 40-51 https://doi.org/10.1016/j.cose.2017.01.004

[4] Odebade, Adejoke T., and Elhadj Benkhelifa. "Evaluating the impact of government Cyber Security initiatives in the UK." *arXiv preprint arXiv:2303.13943* (2023). https://doi.org/10.48550/arXiv.2303.13943

[5] Legg, Philip A., Oliver Buckley, Michael Goldsmith, and Sadie Creese. "Automated insider threat detection system using user and role-based profile assessment." *IEEE Systems Journal* 11, no. 2 (2015): 503-512. https://doi.org/10.1109/JSYST.2015.2438442

[6] Farid, Marina, Rania Elgohary, Ibrahim Moawad, and Mohamed Roushdy. "User profiling approaches, modelling, and personalization." In *Proceedings of the 11th international conference on informatics & systems (INFOS 2018)*. 2018. https://doi.org/10.2139/ssrn.3389811

[7] Cletus, Azaabi, Benjamin Weyory, and Alex Opoku. "Improving social engineering awareness, training and education (SEATE) using a behavioral change model." *International Journal of Advanced Computer Science and Applications* 13, no. 5 (2022). https://doi.org/10.14569/IJACSA.2022.0130572

[8] Sarker, Iqbal H., Helge Janicke, Leandros Maglaras, and Seyit Camtepe. "Data-driven intelligence can revolutionize today's cybersecurity world: A position paper." In *International Conference on Advanced Research in Technologies,*

Information, Innovation and Sustainability, pp. 302-316. Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-48855-9_23

[9] Jalil, Masita, Noraida Hj Ali, Farizah Yunus, Fakhrul Adli Mohd Zaki, Lee Hwee Hsiung, and Mohammed Amin Almaayah. "Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 37, no. 1 (2024): 115-127. https://doi.org/10.37934/araset.37.1.115127

[10] Li, Ling, Wu He, Li Xu, Ash Ivan, Mohd Anwar, and Xiaohong Yuan. "Does explicit information security policy affect employees' cyber security behavior? A pilot study." In *2014 Enterprise systems conference*, pp. 169-173. IEEE, 2014. https://doi.org/10.1109/ES.2014.66

[11] Evans, Mark, Leandros A. Maglaras, Ying He, and Helge Janicke. "Human behaviour as an aspect of cybersecurity assurance." *Security and Communication Networks* 9, no. 17 (2016): 4667-4679. https://doi.org/10.1002/sec.1657

[12] Selvam, Visahl Samson David. "Human error in IT security." *arXiv preprint arXiv:2005.04163* (2020). https://doi.org/10.48550/arXiv.2005.04163

[13] Ifinedo, Princely. "Roles of Social and Organizational Climate Factors in Discouraging Employee Engagement in Nonmalicious Counterproductive Computer Security Behaviors." (2020).. 1

[14] Corradini, Isabella, and Isabella Corradini. "Security: human nature and behaviour." *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology* (2020): 23-47. https://doi.org/10.1007/978-3-030-43999-6_2

[15] Uchendu, Betsy, Jason RC Nurse, Maria Bada, and Steven Furnell. "Developing a cyber security culture: Current practices and future needs." *Computers & Security* 109 (2021): 102387. https://doi.org/10.1016/j.cose.2021.102387

[16] Halim, Izzah Inani Abdul, Alya Geogiana Buja, Mohd Shah Shafie Idris, and Nurul Jannah Mahat. "Implementation of BYOD Security Policy in Malaysia Institutions of Higher Learning (MIHL): An Overview." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 33, no. 2 (2023): 1-14. https://doi.org/10.37934/araset.33.2.114

[17] Evans, Mark, Leandros A. Maglaras, Ying He, and Helge Janicke. "Human behaviour as an aspect of cybersecurity assurance." *Security and Communication Networks* 9, no. 17 (2016): 4667-4679. https://doi.org/10.1002/sec.1657

[18] Burns, A. J., Tom L. Roberts, Clay Posey, Rebecca J. Bennett, and James F. Courtney. "Assessing the role of security education, training, and awareness on insiders' security-related behavior: An expectancy theory approach." In *2015 48th Hawaii International Conference on System Sciences*, pp. 3930-3940. IEEE, 2015." https://doi.org/10.1109/HICSS.2015.471

[19] Shamsudin, Nor Natasha Ashira, Saiful Farik Mat Yatin, N. F. M. Nazim, A. W. Talib, Mohammad Afiq Mohamed Sopiee, and F. N. Shaari. "Information security behaviors among employees." *International Journal of Academic Research in Business and Social Sciences* 9, no. 6 (2019): 560-571. https://doi.org/10.6007/IJARBSS/v9-i6/5972

[20] Goo, Jahyun, Myung-Seong Yim, and Dan J. Kim. "A path to successful management of employee security compliance: An empirical study of information security climate." *IEEE Transactions on Professional Communication* 57, no. 4 (2014): 286-308. https://doi.org/10.1109/TPC.2014.2374011

[21] Jiang, Hemin, Aggeliki Tsohou, Mikko Siponen, and Ying Li. "Examining the side effects of organizational Internet monitoring on employees." *Internet Research* 30, no. 6 (2020): 1613-1630. https://doi.org/10.1108/INTR-08-2019-0360

[22] Mills, Jennifer U., Steven MF Stuban, and Jason Dever. "Predict insider threats using human behaviors." *IEEE Engineering Management Review* 45, no. 1 (2017): 39-48. https://doi.org/10.1109/EMR.2017.2667218