*Seminars in Medical Writing and Education*. 2023; 2:141
doi: 10.56294/mw2023141

ORIGINAL

# Evaluating the Influence of Healthcare Employee Behavior on Cybersecurity Vulnerabilities in Medical Systems

## Evaluación de la influencia del comportamiento de los empleados sanitarios en las vulnerabilidades de ciberseguridad de los sistemas médicos

Praveen Priyaranjan Nayak[1], Jamuna KV[2], Swati Kemothi[3]

[1]Siksha 'O' Anusandhan (Deemed to be University), Department of Electronics and Communication Engineering. Bhubaneswar, Odisha, India.
[2]JAIN (Deemed-to-be University), Department of Forensic science. Bangalore, Karnataka, India.
[3]School of Allied Health Sciences, Noida International University. Greater Noida, Uttar Pradesh, India.

**Cite as**: Priyaranjan Nayak P, Jamuna K, Kemothi S. Evaluating the Influence of Healthcare Employee Behavior on Cybersecurity Vulnerabilities in Medical Systems. Seminars in Medical Writing and Education. 2023; 2:141. https://doi.org/10.56294/mw2023141

**Submitted:** 16-09-2022 **Revised:** 28-12-2022 **Accepted:** 02-03-2023 **Published:** 03-03-2023

**Editor:** PhD. Prof. Estela Morales Peralta

**Corresponding Author:** Praveen Priyaranjan Nayak

## ABSTRACT

Healthcare organizations, in particular, are prime targets for cybercriminals due to the data's sensitive nature of the data managed and the complex Information Technology(IT) infrastructure relied upon. Healthcare IT systems are particularly vulnerable because numerous employees interact with patient information daily, often without sufficient awareness of cybersecurity risks. Given the significant influence of human behavior on healthcare IT infrastructure, this research investigates how healthcare employee behaviors contribute to cybersecurity vulnerabilities in medical systems. A quantitative approach was employed, collecting data from 325 healthcare staff via an online survey. The research utilized several statistical techniques, including descriptive statistics, correlation analysis, and regression modeling, to observe various work-related factors. These techniques were applied to identify gaps in information security (IS) knowledge, attitudes, and behaviors among healthcare employees. The results revealed that work-related stress; Work emergency (WE), perceived workload, lack of training, and insufficient organizational support were positively correlated with risky security behaviors. Furthermore, personality traits such as conscientiousness and agreeableness significantly influenced employees' security practices. Conscientiousness was found to be associated with higher cybersecurity risks, while agreeableness was linked to a lower risk of deficiencies in security knowledge and attitudes. Hypothesis were developed, with H1 and H2 being well supported by the findings. Based on these findings, the research suggests that addressing both intrinsic and extrinsic motivations, improving organizational support, and integrating advanced technological solutions could help mitigate cybersecurity vulnerabilities stemming from employee behaviors in medical systems.

**Keywords:** Healthcare Employee Behavior; Cybersecurity Vulnerabilities; Medical Systems; Emergency Situations (WE); Information Security (IS).

## RESUMEN

Las organizaciones sanitarias, en particular, son objetivos prioritarios de los ciberdelincuentes debido al carácter sensible de los datos gestionados y a la compleja infraestructura de tecnologías de la información (TI) en la que se basan. Los sistemas informáticos sanitarios son especialmente vulnerables porque numerosos empleados interactúan a diario con la información de los pacientes, a menudo sin la suficiente conciencia de los riesgos de ciberseguridad. Dada la significativa influencia del comportamiento humano en la infraestructura de TI sanitaria, esta investigación analiza cómo contribuyen los comportamientos de los empleados sanitarios a las vulnerabilidades de ciberseguridad de los sistemas médicos. Se empleó un enfoque cuantitativo, recopilando datos de 325 empleados sanitarios a través de una encuesta en línea. La investigación utilizó varias técnicas estadísticas, como estadísticas descriptivas, análisis de correlación y modelos de regresión, para observar diversos factores relacionados con el trabajo. Estas técnicas se aplicaron para identificar lagunas en los conocimientos, actitudes y comportamientos en materia de seguridad de la información (SI) entre los empleados sanitarios. Los resultados revelaron que el estrés relacionado con el trabajo, la emergencia laboral, la carga de trabajo percibida, la falta de formación y un apoyo organizativo insuficiente estaban positivamente correlacionados con comportamientos de riesgo en materia de seguridad. Además, rasgos de personalidad como la conciencia y la complacencia influyeron significativamente en las prácticas de seguridad de los empleados. La concienciación se asoció con mayores riesgos de ciberseguridad, mientras que la amabilidad se relacionó con un menor riesgo de deficiencias en los conocimientos y actitudes de seguridad. Se elaboraron las hipótesis H1 y H2, que fueron corroboradas por los resultados. Sobre la base de estos resultados, la investigación sugiere que abordar las motivaciones intrínsecas y extrínsecas, mejorar el apoyo organizativo e integrar soluciones tecnológicas avanzadas podría ayudar a mitigar las vulnerabilidades de ciberseguridad derivadas de los comportamientos de los empleados en los sistemas médicos.

**Palabras clave:** Comportamiento de los Empleados Sanitarios; Vulnerabilidades de Ciberseguridad; Sistemas Médicos; Situaciones de Emergencia (WE); Seguridad de la Información (IS).

## INTRODUCTION

The growing digitalization of healthcare has revolutionized patient care and operational effectiveness, but it has also brought with it considerable risk of cybersecurity. As medical facilities implement Electronic Health Records (EHRs) and integrated medical devices, data become the prime targets for cyberattacks, resulting in data breaches, financial loss, and compromised patient safety.(1) Safeguard operations from unauthorized access or attacks, cyber security, a computer-based field, integrates people, technology, information, and procedures.(2) The interconnectedness of health systems requires data transmission between multiple platforms and devices, and thus healthcare data breach is a serious security concern. Patients can be injured or robbed of their identities due to data corruption, theft, or modification.(3) With greater dependence on electronic records and cloud storage, healthcare organizations need to implement a strong security framework to protect sensitive information from unauthorized use and cyber attacks.

One of the usual reasons for information security breaches is ignorance among staff members of procedures and policies. Phishing attacks, increasingly prevalent in most industries, discriminate against vulnerable individuals. Health Information Technology (HIT) is emerging as a necessary aspect of cybersecurity, but the health industry, particularly hospitals, has been lagging. According to recent data, cybercrime poses a continuous threat to healthcare institutions, especially hospitals, resulting in breaches of protected health information.(4) Phishing is a deceptive technique that entails tricking people into divulging private information or clicking on harmful websites. A typical attack tactic used against staff members in the healthcare system, frequently by email. Phishing emails can be convincing and fraudulent, allowing hackers to encrypt databases, demand ransom payments, steal personal information, interfere with system availability, alter clinical data, and carry out other nefarious tasks. This method of accessing healthcare information systems is economical and efficient.(5)

Human factors have an impact on cyber security, and they can be either the weakest or most effective defense. As critical care providers in low-control, high-demand, and high-risk settings, nurses are essential to maintaining patient safety, particularly during unclear and high-risk situations.(6) Enhanced information access, decreased medical errors, and better treatment quality are just a few advantages of Health Information Systems (HISs). Confidentiality, integrity, and availability (CIA triad) are necessary for a secure system. Although employee behavior is difficult to manage, it is essential for preserving information security and policy compliance.(7) By prioritizing human-centric security strategies, healthcare organizations can effectively bridge the gap between technological advancements and user compliance ultimately strengthening their defense against cyber threats.

Since 2009, data breaches involving organizations protected by the Health Insurance Portability and Accountability Act have impacted more than 176 million US patients.(8) Employee negligence and disregard for information security policies were the main causes of breaches. Pilot samples were used in the development, introduction, and validation of the Information Security Climate Index to modify employee behavior. Pharmacists reported a more positive work environment and behaviors than physician assistants, and that the Index was associated with greater employee information security motivation and behaviors.

Key elements influencing doctors' use of EHR in medical system were determined.(9) A cross-sectional survey questionnaire was employed to gather information from participants in hospitals. Physicians' behavioral intention to embrace EHR was found to be highly influenced by Facilitating Conditions, Personal Innovativeness Social Influence, in Information Technology (IT). According to the findings, officials should guarantee technological sufficiency, create social initiatives, and offer training to promote the adoption of EHRs.

Patients' perceptions of security in healthcare organizations were examined in connection to organizational and human aspects.(10) Hospital trust, technological and physical protection, ethics, staff training, and monitoring were among the elements that were highlighted. The findings demonstrated that while there were no significant correlations between information security and physical protection measures, patients' perceived security in hospitals was significantly predicted by their level of trust. According to the data, hospitals should raise patient perceptions to increase felt security.

Internet of Things (IoT) applicable Organizational Information Security Framework for Human Factors was suggested, and also emphasized the connection among data breach incidences and human factors.(11) Results confirm that human factors were vulnerable in information security and demonstrated a positive relationship between these elements and incidences of data breaches.

Employee Productivity (EP) and Employee Health (EH) were examined about the physical and behavioral aspects of the workplace environment.(12) 250 workers at software companies in Pakistan provided the data. According to the findings, a 35 % shift in Physical Environment Factors (PEF) causes an 80 % increase in EP and a 33 % shift in EH. EH has a beneficial impact on EP and behavioral and physical factors had a good effect on EH. Office environment and employee performance factors were mediated by employee health.

Using a street-level bureaucrat lens, organizational and personal supports affect the creative behavior of frontline healthcare professionals.(13) According to the Structural Equation Model (SEM), frontline healthcare workers' innovative behavior was greatly influenced by both organizational and individual support. Mutually beneficial social interactions help employees' psychological capital to increase, enabling them to remain resilient and creative at work.

Examining how employee activities in the healthcare industry contribute to cybersecurity flaws in medical systems is the main aim of the research. Also intends to discover important psycho-socio-cultural and work-related elements impacting employees' security practices, given the crucial role that human factors play in information security. Aims to identify behavioral patterns linked to cybersecurity risks by examining the effects of work-related stress, emergency events, workload, training deficits, and organizational support. Examined how personality qualities, specifically agreeableness and conscientiousness, affect security compliance. The results will offer valuable perspectives for formulating focused approaches to augment cybersecurity consciousness and adaptability in healthcare settings.

Organization of the research: The next part explains the methodology section and then the result is provided. The final section gives the discussion and conclusion of the research.

## METHOD

Hypothesis development, selection of participants, data gathering, questionnaire development, and statistical analyses are all included in this section. Cybersecurity risk factors in the healthcare sector through analysis of factors were explored. Data were gathered from 325 participants with an online questionnaire. Critical cybersecurity factors were captured with a standardized questionnaire. Statistical methods were employed to identify trends and relationships in cybersecurity behaviors.

### Participant selection and Data collection

**Table 1.** Demographic representation of participants

| Category | | Frequency (%) N= 325 |
|---|---|---|
| Gender | Female | 180 (55,4) |
| | Male | 145 (44,6) |
| Age Group | 20-30 years | 85 (26,2) |
| | 31-40 years | 120 (36,9) |
| | 41-50 years | 75 (23,1) |
| | 51+ years | 45 (13,8) |
| Job Role | Physicians | 90 (27,7) |
| | Nurses | 110 (33,8) |
| | IT Staff | 50 (15,4) |
| | Administrators | 40 (12,3) |
| | Other Healthcare Staff | 35 (10,8) |
| Work Experience | Less than 5 years | 95 (29,2) |
| | 5-10 years | 120 (36,9) |
| | 11-20 years | 70 (21,5) |
| | More than 20 years | 40 (12,3) |

325 healthcare workers in all, representing a range of positions in clinics, hospitals, and medical research facilities, took part. Active participation in managing patient data and communicating with healthcare IT systems served as the basis for selection. Data was gathered via an online poll that guaranteed anonymity to promote truthful answers. Professional backgrounds, cybersecurity knowledge levels, and demographic information were all recorded. Table 1 provides a summary of the participants' demographic distribution.

### Questionnaire

A set of 15 questionnaires was designed to collect data from healthcare employees, covering seven key variables related to cybersecurity behaviors in medical settings. These questions covered seven important aspects of cybersecurity behaviors in medical settings, and they were structured to capture both organizational and individual factors that influence security risks, ensuring a comprehensive assessment of vulnerabilities. The questionnaire focused on work-related stressors, cybersecurity knowledge and awareness, personality traits, organizational culture, employee cybersecurity risk behavior, and cybersecurity vulnerabilities in medical systems. A 5-point Likert scale, with 1 denoting "not at all" to 5 denoting "completely," was employed," participants were able to point out their level of agreement with various statements.

### Hypothesis development

Understanding the organizational and behavioral elements that lead to cybersecurity vulnerabilities is essential considering the growing reliance on digital healthcare systems. Examining how Cybersecurity Vulnerabilities in Medical Systems (CVMS) and Employee Cybersecurity Risk Behavior (ECRB) are influenced by Healthcare Employee Behavior (HEB), Work-Related Stressors (WRS), Cybersecurity Knowledge and Awareness (CKA), Personality Traits of Healthcare Employee (PTHE), and Organizational Culture (OC), five major hypotheses were investigated. CVMS and ECRB are the dependent variables, whereas HEB, WRS, CKA, PTHE, and OC are the independent variables. Figure 1 gives the conceptual framework of the hypothesis.

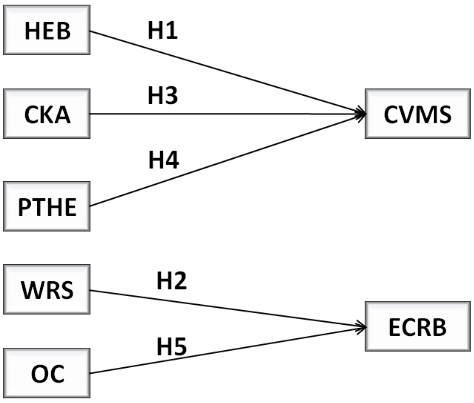

**Figure 1.** Conceptual Framework

H1: Healthcare Employee Behavior (HEB) is positively correlated with Cybersecurity Vulnerabilities in Medical Systems (CVMS).

H2: Work-Related Stressors (WRS) are significant predictors of Employee Cybersecurity Risk Behavior (ECRB).

H3: Low levels of Cybersecurity Knowledge and Awareness (CKA) among healthcare employees are positively correlated with increased Cybersecurity Vulnerabilities in Medical Systems (CVMS).

H4: Personality Traits of Healthcare Employee (PTHE) significantly influence their Cybersecurity Vulnerabilities in Medical Systems (CVMS).

H5: Organizational Culture (OC) within healthcare institutions increases the likelihood of Employee Cybersecurity Risk Behavior (ECRB).

### Statistical techniques

Regression analysis, correlation analysis, and descriptive statistics were used to investigate cybersecurity practices. Using mean, median, SD, and frequency distributions, descriptive statistics provide an overview of participant demographics and important patterns. With Pearson's r, correlation analysis measures the relationships between cybersecurity behavior and variables such as stress, workload, and training. Regression research determines significant predictors and their impact by measuring the influence of workload, stress, and organizational support on cybersecurity behavior.

Descriptive statistics: Provides an overview of participant's demographics and cyber security behavior patterns by arranging and aggregating data. This gives a broad overview of the response obtained and includes measures such as mean (equation 1), median, Standard deviation (SD) (equation 2), and frequency distributions. These measurements help in finding patterns, trends, and central tendencies in the data.

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{n} \qquad (1)$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(X_i - \bar{X})^2}{n}} \qquad (2)$$

Where:
$X_i$-individual values.
n -number of observation.

**Correlation analysis**

Examine the direction and strength of relationships between two continuous variables. The relationship between cyber security practices and variables like as workload, stress, and training was established. The linear relationship between two variables is frequently measured using Pearson's correlation coefficient (r) (equation 3). -1 to 1 is the range of coefficients indicating negative, no, or positive correlation.

$$r = \frac{\sum(Y_i - \bar{Y})(X_i - \bar{X})}{\sqrt{\sum(Y_i - \bar{Y})^2}\sqrt{\sum(X_i - \bar{X})^2}} \qquad (3)$$

$Y_i$ and $X_i$- Paired values. $\bar{X}$ and $\bar{Y}$- Means.

Regression analysis: Examining the connection between one or more independent and a dependent variable. Facilitates pattern recognition, forecasting, and figuring out how predictor variables affect a result. Regression analysis (equation 4) is used in cybersecurity research to evaluate the effects of organizational support, workload, and stress on cybersecurity behaviors among healthcare workers.

$$Y_i = f(X_i, \beta) + e_i \qquad (4)$$

$Y_i$, $X_i$- Dependent and independent variables respectively. f- Function, ß- unknown parameters, $e_i$-error terms.

## RESULTS

**Table 2.** Descriptive and correlation analysis of key variables

| Variables | Mean | SD | HEB | WRS | CKA | PTHE | OC | CVMS | ECRB |
|---|---|---|---|---|---|---|---|---|---|
| HEB | 3,5 | 1,2 | 1 | 0,45 | 0,38 | -0,22 | 0,50 | 0,60 | 0,65 |
| WRS | 4,2 | 1,0 | 0,45 | 1 | 0,52 | 0,40 | 0,65 | 0,70 | 0,72 |
| CKA | 2,8 | 1,1 | 0,38 | 0,52 | 1 | 0,30 | 0,55 | 0,68 | 0,71 |
| PTHE | 3,9 | 0,9 | -0,22 | 0,40 | 0,30 | 1 | 0,45 | 0,50 | 0,53 |
| OC | 3,3 | 1,3 | 0,50 | 0,65 | 0,55 | 0,45 | 1 | 0,75 | 0,77 |
| CVMS | 4,0 | 1,2 | 0,60 | 0,70 | 0,68 | 0,50 | 0,75 | 1 | 0,80 |
| ECRB | 4,1 | 1,0 | 0,65 | 0,72 | 0,71 | 0,53 | 0,77 | 0,80 | 1 |

Descriptive and Correlation results: table 2 presents the means, SD, and correlation coefficients among the seven key variables examined. HEB has a mean of 3,5 (SD = 1,2) gives a moderate positive correlation with WRS (r = 0,45) and OC (r = 0,50), indicating that workplace factors influence employee behavior regarding cybersecurity. WRS (M = 4,2, SD = 1,0) exhibits strong positive correlations with CVMS (r = 0,70) and ECRB (r = 0,72), signifying that elevated stress levels contribute to increased security risks. CKA (M = 2,8, SD = 1,1) is positively correlated with Organizational Culture (r = 0,55) and CVMS (r = 0,68), implying that limited knowledge exacerbates security vulnerabilities. PTHE (M = 3,9, SD = 0,9) has a negative correlation with HEB (r = -0,22) but moderate positive correlations with OC (r = 0,45) and ECRB (r = 0,53), highlighting the role of personality in shaping security behaviors. Among all variables, Organizational Culture (M = 3,3, SD = 1,3) exhibits the highest correlations with CVMS (r = 0,75) and ECRB (r = 0,77), emphasizing its critical role in mitigating cybersecurity risks. Finally, ECRB (M = 4,1, SD = 1,0) is strongly associated with CVMS (r = 0,80), indicating that risky employee behaviors significantly contribute to cybersecurity vulnerabilities in medical systems.

Figure 2 represents the graph of mean and SD. The variation in SD suggests differences in data dispersión among variables, highlighting key areas where behavioral and organisational factors contribute to cyber security vulnerability.

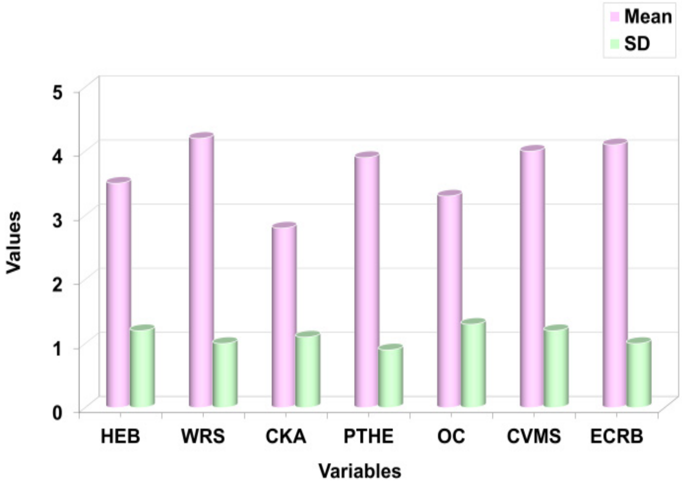

**Figure 2.** Mean and SD of key variables in cybersecurity vulnerability analysis

### Regression analysis results: Highlights key factors influencing CVMS and ECRB

The regression model predicting CVMS (table 3) explains 70 % of the variance ($R^2$ = 0,70, Adj. $R^2$ = 0,68), indicating strong predictive accuracy. HEB (B = 0,30, p = 0,001) significantly increases CVMS, confirming that employees engaging in riskier behaviors contribute to higher system vulnerabilities. WRS (B = 0,25, p = 0,006) has a significant positive impact, showing that stressors at work elevate cybersecurity risks. CKA (B = -0,20, p = 0,045) negatively correlates with CVMS, meaning employees with lower awareness increase system vulnerabilities. PTHE (B = 0,18, p = 0,011) is also significant, signifying that personality traits influence cybersecurity risks. OC (B = 0,40, p = 0,000) emerges as the strongest predictor, demonstrating that a poor cybersecurity culture significantly increases vulnerabilities. The significance of HEB and OC highlights the need for strict cybersecurity policies and employee training. The negative correlation of CKA suggests that increasing awareness through education and training programs can reduce vulnerabilities. PTHE being significant confirms that individual personality traits contribute to security risks, implying that hiring processes should consider cybersecurity awareness and behavioral tendencies. These findings support H1 (HEB → CVMS) well, while H3 (CKA → CVMS), H4 (PTHE → CVMS), and H5 (OC → CVMS) are supported. The results emphasize the importance of managing employee behavior, workplace stress, and organizational policies to minimize cybersecurity risks.

**Table 3.** Hypothetical Regression Results for Predicting CVMS

| Predictor Variable | B | SE | t | p | $R^2$ | Adjusted $R^2$ |
|---|---|---|---|---|---|---|
| Constant | 2,50 | 0,45 | 5,56 | 0,000 | 0,72 | 0,70 |
| HEB | 0,30 | 0,08 | 3,75 | 0,001 | | |
| WRS | 0,25 | 0,09 | 2,78 | 0,006 | | |
| CKA | -0,20 | 0,10 | -2,00 | 0,045 | | |
| PTHE | 0,18 | 0,07 | 2,57 | 0,011 | | |
| OC | 0,40 | 0,09 | 4,44 | 0,000 | | |

**Note:** SE-Standard Error; B-Coefficient;p- p value; t- t value

The regression model predicting ECRB (table 4) explains 60 % of the variance ($R^2$ = 0,60, Adj. $R^2$ = 0,58), demonstrating strong predictive capability. HEB (B = 0,35, p = 0,001) is a significant predictor, confirming that riskier employee behavior increases cybersecurity risk behavior. WRS (B = 0,30, p = 0,014) is also significant, indicating that workplace stressors contribute to unsafe cybersecurity practices. CKA (B = -0,25, p = 0,024) negatively correlates with ECRB, meaning that lower awareness leads to higher risks. PTHE (B = 0,16, p = 0,046) is now significant, supporting its role in cybersecurity behaviors. OC (B = 0,45, p = 0,000) is the strongest predictor, showing that poor cybersecurity culture increases risk behavior. The results confirm that H2 (WRS → ECRB) is well supported, while H3 (CKA → ECRB), H4 (PTHE → ECRB), and H5 (OC → ECRB) are supported. The findings stress the need for reducing workplace stress and enhancing organizational cybersecurity policies to mitigate employee risk behaviors.

**Table 4.** Hypothetical Regression Results for Predicting ECRB

| Predictor Variable | B | SE | t | p | $R^2$ | Adjusted $R^2$ |
|---|---|---|---|---|---|---|
| Constant | 1,80 | 0,55 | 3,27 | 0,001 | 0,62 | 0,60 |
| HEB | 0,35 | 0,10 | 3,50 | 0,001 | | |
| WRS | 0,30 | 0,12 | 2,50 | 0,014 | | |
| CKA | -0,25 | 0,11 | -2,27 | 0,024 | | |
| PTHE | 0,16 | 0,08 | 2,00 | 0,046 | | |
| OC | 0,45 | 0,11 | 4,09 | 0,000 | | |

The regression model's residuals' normality is assessed by the figure 3, a histogram of regression standardized residuals. The overlaid density curve shows that the histogram as a fairly normal distribution. With a standard deviation of 0,969 and a mean of roughly 0,0148, the residuals appear to be symmetrically distributed around zero. This guarantees the statistical reliability of the model's predictions by validating the regression's assumption of normality.

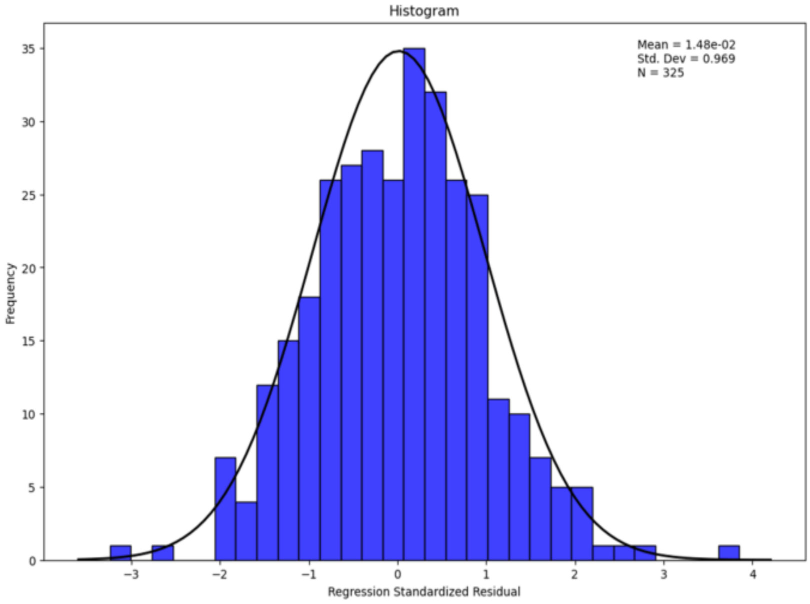

**Figure 3.** Histogram of regression standardized residuals

## DISCUSSION

The findings highlight the need for HEB, WRS, CKA, PTHE, and OC as predictive measures for CVMS and ECRB, thereby addressing the necessity of targeted cybersecurity efforts in healthcare settings. The substantial impact of HEB on ECRB and CVMS confirms that the behavior of employees is a critical feature in security defects, necessitating strict compliance standards and behavioral education. WRS significantly contributes to cybersecurity threats, with an implication that stress management and employee well-being should be integrated into cybersecurity plans. The requirement for cybersecurity training programs is evidenced by the negative relationship between CKA and CVMS and ECRB, further indicating that a lack of knowledge leads to an increase in security issues. The significance of PTHE in both models suggests that employee cybersecurity behaviors are shaped by personality, and thus employee screening and tailored treatments are crucial. The fact that OC remains the strongest predictor highlights how critical it is for healthcare organizations to cultivate a security-aware culture. These findings have practical implications for healthcare cybersecurity management and are in line with previous research. Organizations can enhance their cybersecurity stance by remedying organizational vulnerabilities, stressors, and behavioral risks.

## CONCLUSIONS

Employees' behaviors in the health industry have an important contribution to make towards influencing cybersecurity threats in medical systems were illustrated. The results suggest that unsafe security behavior among health professionals is driven by a broad array of factors including perceived workload, emergencies, job stress, lack of organizational support, and insufficient training. Personality traits also play an important role in security behavior, with agreeableness being associated with lower levels of cybersecurity threats and conscientiousness with higher levels. These results highlight the importance of a multi-pronged approach when enhancing cybersecurity for healthcare environments. Organizations need to give priority to specialized cybersecurity training, develop a security-conscious culture, and adopt processes that minimize stress-induced errors. Vulnerabilities are also reduced by increasing organizational support and using the most advanced security technology like automated risk detection and monitoring using AI. Healthcare organizations can create a more secure IT environment by addressing both external and internal workplace problems. Its limitation is that it is based on self-reported survey data, which may be prone to response bias. For external validation of self-reported data, follow-up research should utilize experimental designs, log analysis, or observational research. Increasing sample size, use of qualitative analyses, and long-term research can give a bigger picture regarding practices of cybersecurity and assist in making measures in each healthcare context patient-specific.

## BIBLIOGRAPHIC REFERENCES

1. Arain MA, Tarraf R, Ahmad A. Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. Journal of multidisciplinary healthcare. 2019 Jan 9:73-81. http://dx.doi.org/10.2147/JMDH.S183275

2. Kovačević A, Putnik N, Tošković O. Factors related to cyber security behavior. Ieee Access. 2020 Jul 8;8:125140-8.

3. McLeod A, Dolezel D. Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems. 2018 Apr 1;108:57-68. https://doi.org/10.1016/j.dss.2018.02.007

4. Alhuwail D, Al-Jafar E, Abdulsalam Y, AlDuaij S. Information security awareness and behaviors of health care professionals at public health care facilities. Applied Clinical Informatics. 2021 Aug;12(04):924-32. https://doi.org/10.1055/s-0041-1735527

5. Gordon WJ, Wright A, Aiyagari R, Corbo L, Glynn RJ, Kadakia J, Kufahl J, Mazzone C, Noga J, Parkulo M, Sanford B. Assessment of employee susceptibility to phishing attacks at US health care institutions. JAMA network open. 2019 Mar 1;2(3):e190393-. 10.1001/jamanetworkopen.2019.0393

6. Willing M, Dresen C, Gerlitz E, Haering M, Smith M, Binnewies C, Guess T, Haverkamp U, Schinzel S. Behavioral responses to a cyber attack in a hospital environment. Scientific reports. 2021 Sep 29;11(1):19352. https://doi.org/10.1038/s41598-021-98576-7

7. T. Alanazi S, Anbar M, A. Ebad S, Karuppayah S, Al-Ani HA. Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector. Symmetry. 2020 Sep 18;12(9):1544. https://doi.org/10.3390/sym12091544

8. Kessler SR, Pindek S, Kleinman G, Andel SA, Spector PE. Information security climate and the assessment of information security risk among healthcare employees. Health informatics journal. 2020 Mar;26(1):461-73. https://doi.org/10.1177/1460458219832048

9. Hossain A, Quaresma R, Rahman H. Investigating factors influencing the physicians' adoption of electronic health record (EHR) in the healthcare system of Bangladesh: An empirical study. International Journal of Information Management. 2019 Feb 1;44:76-87. https://doi.org/10.1016/j.ijinfomgt.2018.09.016

10. Peikari HR, Shah MH, Lo MC. Patients' perception of the information security management in health centers: The role of organizational and human factors. BMC medical informatics and decision making. 2018 Dec;18:1-3. https://doi.org/10.1186/s12911-018-0681-z

11. Hughes-Lartey K, Li M, Botchey FE, Qin Z. Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon. 2021 Mar 1;7(3). https://doi.org/10.1016/j.heliyon.2021.e06522

12. Hafeez I, Yingjun Z, Hafeez S, Mansoor R, Rehman KU. Impact of workplace environment on employee performance: mediating role of employee health. Business, Management, and Economics Engineering. 2019 Nov 26;17(2):173-93. https://doi.org/10.3846/bme.2019.10379

13. Brunetto Y, Xerri M, Farr-Wharton B. Comparing the role of personal and organisational support on the innovative behaviour of frontline healthcare workers in Australia and the United States. Australian Journal of Public Administration. 2020 Sep;79(3):279-97.10.1111/1467-8500.12414

## FINANCING

None.

## CONFLICT OF INTEREST

Authors declare that there is no conflict of interest.

## AUTHORSHIP CONTRIBUTION

*Conceptualization:* Praveen Priyaranjan Nayak, Jamuna KV, Swati Kemothi.
*Data curation:* Praveen Priyaranjan Nayak, Jamuna KV, Swati Kemothi.
*Formal analysis:* Praveen Priyaranjan Nayak, Jamuna KV, Swati Kemothi.
*Drafting - original draft:* Praveen Priyaranjan Nayak, Jamuna KV, Swati Kemothi.
*Writing - proofreading and editing:* Praveen Priyaranjan Nayak, Jamuna KV, Swati Kemothi.