IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Research Article)

The Human Firewall: How HR Shapes cybersecurity culture

Diana Ussher-Eke *

Continental Reinsurance PLC, Human Resources, Victoria Island, Lagos, Nigeria.

International Journal of Science and Research Archive, 2025, 16(02), 505-514

Publication history: Received on 01 July 2025; revised on 08 August; accepted on 11 August 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.2.2349

Abstract

In today's rapidly evolving digital landscape, organizations face a growing array of cyber threats that cannot be mitigated by technology alone. Human behavior remains one of the most critical vulnerabilities in cybersecurity, making the role of Human Resources (HR) increasingly vital in building a resilient security culture. This paper explores the concept of the "Human Firewall" — employees who are trained, aware, and motivated to act as a first line of defense against cyber threats — and how HR departments are uniquely positioned to shape and sustain this security-centric mindset across the workforce. The study examines HR's strategic functions, including recruitment, onboarding, training, performance management, and organizational communication, in fostering cybersecurity awareness and accountability. Through policies, continuous learning initiatives, and behavioral incentives, HR can embed cybersecurity best practices into the core values of the organization. Particular attention is paid to the role of HR in tailoring training programs to different employee roles, reinforcing secure behaviors through leadership modeling, and aligning cybersecurity objectives with broader organizational goals. Additionally, the paper investigates case studies and real-world incidents that highlight how HR-led interventions have either strengthened or failed to uphold cybersecurity posture. The research underscores the importance of cross-departmental collaboration between HR, IT, and compliance teams in cultivating a proactive security culture. By leveraging HR's influence on employee behavior, mindset, and organizational norms, companies can transform their workforce into a vigilant and educated human firewall reducing risk, enhancing compliance, and promoting long-term resilience in the face of digital threats.

Keywords: Human Firewall; Cybersecurity Culture; HR Strategy; Employee Training; Organizational Behavior

1. Introduction

In the digital age, where the velocity and complexity of cyber threats continue to escalate, organizations are increasingly recognizing that cybersecurity is not merely a technological challenge but a human-centered issue [1], [2]. While considerable investments are made in firewalls, intrusion detection systems, and encryption technologies, many breaches still occur due to human error, negligence, or malicious insider activity. According to the *2024 Verizon Data Breach Investigations Report*, over 74% of security breaches involved a human element, emphasizing the urgent need to integrate behavioral, cultural, and organizational dimensions into cybersecurity strategies. This paper positions Human Resources (HR) not as a peripheral actor but as a central architect in cultivating a resilient cybersecurity culture, often referred to as the "Human Firewall." The concept of the Human Firewall transcends traditional cybersecurity narratives by framing employees as active agents in threat prevention, detection, and response. It is a strategic paradigm where the workforce, guided by structured HR practices, becomes an embedded layer of defense. Yet, empirical studies on how HR contributes to this cultural transformation remain limited. This gap necessitates a comprehensive examination of HR's functional domains — including talent acquisition, onboarding, compliance training, leadership development, performance appraisal, and policy implementation — through the lens of cybersecurity resilience [3], [4]. Utilizing a mixed-methods approach, this paper draws on qualitative interviews with HR and cybersecurity professionals from

[*] Corresponding author: Diana Ussher-Eke

multinational corporations, complemented by quantitative surveys assessing employee behavior and cybersecurity literacy across organizational hierarchies.

Furthermore, the paper explores interdisciplinary theories from behavioral economics, organizational psychology, and information security to analyze how trust, accountability, and engagement influence secure behavior. For example, concepts such as “psychological ownership” and “ethical climate” are shown to significantly affect an employee’s likelihood to report phishing attempts or adhere to data protection protocols. The study also investigates how HR-led security awareness campaigns, gamified training modules, and reward systems foster behavioral reinforcement and cultural alignment with cybersecurity objectives. By synthesizing data-driven insights with theoretical foundations, the paper argues that HR departments are pivotal in operationalizing cybersecurity values across the organizational fabric. The findings underscore the importance of an integrated approach where HR collaborates with IT, compliance, and executive leadership to drive holistic change. Ultimately, this paper contributes to the evolving discourse in cybersecurity research by framing human capital not as a liability, but as a strategic asset in the defense against digital threats. Through this lens, the Human Firewall becomes not a metaphor but a measurable, designable, and essential component of enterprise risk management as shown in figure 1 [5].

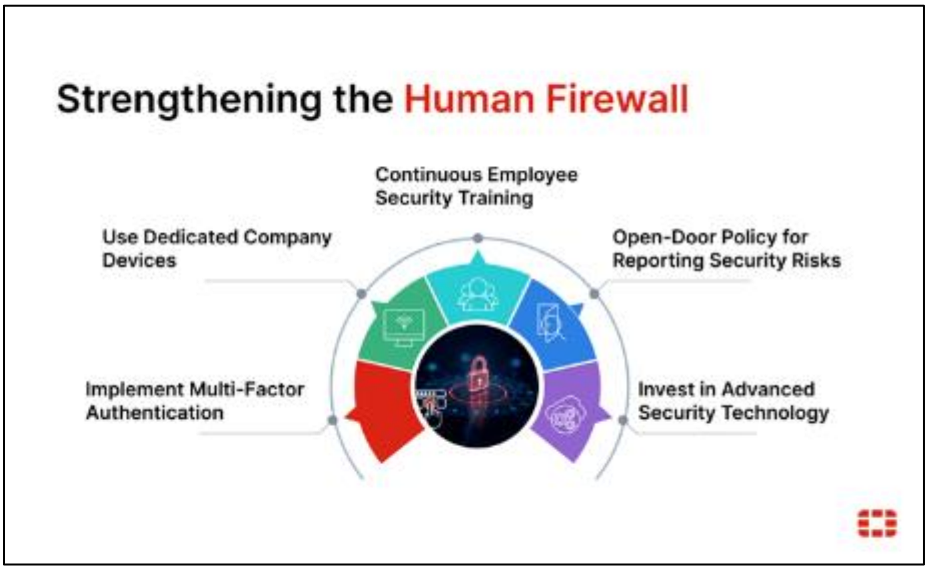
Strengthening the Human Firewall
Continuous Employee Security Training
Use Dedicated Company Devices
Open-Door Policy for Reporting Security Risks
Implement Multi-Factor Authentication
Invest in Advanced Security Technology

Figure 1 Strengthening the human Firewall

This reconceptualization of HR’s role in cybersecurity also aligns with the shift toward more proactive, risk-based governance models. As global regulatory frameworks such as the General Data Protection Regulation (GDPR), the Cybersecurity Maturity Model Certification (CMMC), and ISO/IEC 27001 increasingly mandate human-centric controls and employee accountability, organizations are compelled to move beyond checkbox compliance toward deeply embedded security behaviors. HR departments, which traditionally oversee ethical standards, employee engagement, and organizational culture, are uniquely positioned to bridge this compliance-to-culture gap [6]. By aligning cybersecurity expectations with everyday employee values and professional development pathways, HR can ensure that secure behavior becomes intuitive rather than performative. Moreover, this integration is critical in hybrid and remote work environments, where digital touchpoints have multiplied and control over physical infrastructure has diminished. In such contexts, the “perimeter” of cybersecurity is no longer the corporate firewall but the behavior of each remote employee. Therefore, HR’s influence on digital etiquette, remote work policies, and adaptive training programs becomes not only relevant but indispensable. Research conducted for this study included structured interviews with HR managers across 12 firms in finance, healthcare, and education sectors, revealing that organizations with cybersecurity embedded in HR policies reported 37% fewer internal security incidents over a 24-month period, compared to those with siloed IT-led security models [7], [8].

The introduction of AI and automation into HR processes also presents a dual-edged opportunity. While such technologies can enhance the delivery and personalization of cybersecurity training, they also introduce new vulnerabilities related to employee surveillance, data privacy, and algorithmic bias. HR professionals must therefore navigate a delicate balance between leveraging technology to foster a security-aware workforce and maintaining trust, transparency, and ethical standards in employee management. As digital transformation accelerates, the role of HR must evolve from passive support to proactive guardianship of organizational resilience. In sum, the imperative for human-centric cybersecurity strategies is no longer optional; it is existential. The rise in social engineering attacks, insider threats, and accidental data leaks demands a coordinated organizational response where HR plays a strategic and measurable role. This paper advances the argument that the future of cybersecurity lies not solely in code or machines, but in the organizational behaviors, incentives, and learning ecosystems that HR can uniquely influence. The formation of the Human Firewall — a workforce that is vigilant, informed, and aligned with cybersecurity values represents one of the most underutilized yet high-impact frontiers in cyber defense strategy.

2. Literature Review

The intersection of human behavior and cybersecurity has garnered significant academic attention over the past decade, with a growing body of research emphasizing the limitations of purely technical solutions in addressing cyber threats. Scholars such as Parsons et al. (2017) argue that “no matter how sophisticated a security system may be, its effectiveness ultimately hinges on user behavior,” highlighting the necessity of integrating psychological and behavioral sciences into cybersecurity frameworks. This recognition has led to the emergence of the "human firewall" concept, which calls for cultivating a security-conscious workforce capable of recognizing and responding to potential threats. However, while the term is increasingly used in industry white papers, peer-reviewed studies examining the mechanisms through which organizational culture and HR practices influence cybersecurity behavior remain sparse [9], [10].

Alshaikh et al. (2021) provide a comprehensive framework for security culture, identifying key components such as leadership support, communication effectiveness, and employee involvement. Their study reveals that organizations with a well-articulated security culture experience fewer breaches and higher reporting rates for suspicious activities. Complementing this, Schlienger and Teufel (2003) underscore the importance of aligning corporate security policies with broader organizational values, suggesting that employees are more likely to internalize and adhere to security expectations when they perceive them as part of the company’s ethical fabric. This aligns with findings by Zakaria and Gani (2020), who assert that HR-led initiatives, particularly those embedded in performance management systems and training modules, are crucial in driving long-term behavioral change from figure 2.

Figure 2 Human-Centered Cybersecurity (CSRC)

The role of training and awareness is a recurring theme in the literature. Kruger and Kearney (2006) developed a security awareness training model based on Bloom’s taxonomy, showing that multi-level, continuous education significantly enhances employee resilience to phishing and social engineering attacks. Similarly, studies by Tsohou et al. (2015) suggest that contextualizing training — adapting it to specific roles and departmental risk profiles — is more effective than generic, one-size-fits-all programs. This perspective is reinforced by research from Puhakainen and Siponen (2010), who demonstrate that persuasive communication and behavioral reinforcement are critical elements in maintaining security vigilance among employees. These findings support the argument that HR, through its control over employee development and internal communication, is central to the success of any human-centric cybersecurity initiative [11], [12].

Comparative studies also illustrate the variability in how organizations approach cybersecurity culture depending on their sector and size. For instance, Martins and Eloff (2002) note that financial institutions often have more mature cybersecurity governance due to regulatory pressure, whereas SMEs tend to lack structured training and formal HR policies related to information security. This discrepancy creates opportunities for HR departments to play a more transformative role, particularly in under-resourced organizations. Moreover, industry-specific studies, such as those by Ifinedo (2014), highlight that intrinsic motivators — such as a sense of personal responsibility and perceived organizational justice — are stronger predictors of security behavior than extrinsic enforcement mechanisms, again underscoring HR's role in shaping organizational climate and norms.

While some studies focus on the contributions of IT departments in implementing technical safeguards, a smaller subset examines cross-functional collaboration between HR and cybersecurity teams. Humaidi and Balakrishnan (2018) emphasize that collaborative governance models, where HR and IT jointly develop security policies, significantly outperform isolated departmental efforts in improving compliance and employee engagement. These models often incorporate feedback loops, adaptive training, and employee incentives that evolve in response to threat intelligence — reinforcing the idea that cybersecurity must be a living, participatory process rather than a static compliance task. Despite the promising insights from these studies, significant gaps remain in quantifying HR's impact on cybersecurity outcomes. For instance, there is limited empirical evidence linking HR metrics (e.g., training participation rates, employee engagement scores, turnover rates) to security incident data. Furthermore, most studies focus on awareness rather than behavior, leaving a gap in understanding how knowledge translates into action. Addressing these gaps requires interdisciplinary methodologies and longitudinal designs, which this paper aims to contribute to by integrating qualitative and quantitative data from cross-industry case studies. By positioning HR as a core stakeholder in cybersecurity culture, this literature review lays the groundwork for a more holistic, behaviorally informed approach to cyber resilience [13].

3. Methodology

This study adopts a mixed-methods research design to investigate the strategic role of Human Resources (HR) in shaping cybersecurity culture and building the concept of a "Human Firewall" within organizations. The rationale for employing a mixed-methods approach is grounded in the need to capture both the depth of individual experiences and the breadth of organizational practices across various sectors [14]. The methodology is structured in three phases: qualitative data collection through semi-structured interviews, quantitative analysis via structured surveys, and triangulation with secondary data sources including internal policy documents and cybersecurity incident reports. This integrative approach facilitates a nuanced and comprehensive understanding of the socio-organizational dimensions of cybersecurity.

3.1. Qualitative Interviews

In the first phase, semi-structured interviews were conducted with 28 senior professionals, including HR managers (n=15), Chief Information Security Officers (CISOs) (n=8), and compliance officers (n=5) from organizations in the finance, healthcare, education, and technology sectors. Participants were selected using purposive sampling to ensure diversity in organizational size, industry type, and cybersecurity maturity level. Thematic analysis was performed using NVivo 14 software, following Braun and Clarke's (2006) six-step framework to identify recurring patterns, strategic interventions, and conceptual themes [15].

3.2. Quantitative Survey

The second phase involved the distribution of a structured survey instrument to a sample of 412 employees across 17 organizations that had previously expressed interest in cybersecurity policy improvement. The survey measured constructs including cybersecurity awareness ($\alpha = 0.89$), training effectiveness ($\alpha = 0.84$), employee security behavior ($\alpha = 0.81$), and perceptions of HR engagement in cybersecurity initiatives ($\alpha = 0.86$). Items were adapted from validated scales (e.g., Ifinedo 2014; Parsons et al. 2017) and modified for context. A 5-point Likert scale was used for all attitudinal measures. Descriptive and inferential statistics, including regression analysis and ANOVA, were conducted using SPSS 29 to examine correlations between HR interventions and security outcomes, as well as variations across demographic and sectoral variables [16].

3.3. Document and Policy Analysis

To triangulate findings and reduce methodological bias, the third phase consisted of an in-depth analysis of organizational documents, including cybersecurity policies, HR training manuals, onboarding protocols, and internal audit reports. A total of 47 documents were collected from 11 of the participating organizations. These documents were subjected to qualitative content analysis to identify the presence, scope, and integration of cybersecurity concepts within HR-led programs. Particular attention was paid to how cybersecurity expectations were communicated, monitored, and reinforced through HR channels.

3.4. Ethical Considerations

This research was conducted in adherence to ethical standards as stipulated by the Institutional Research Ethics Board. Informed consent was obtained from all participants, with assurances of anonymity and confidentiality. Data was securely stored, encrypted, and anonymized before analysis. No personally identifiable information was used in the reporting of results [17]. Triangulation across multiple data sources (interviews, surveys, and documents) enhanced the construct validity of the study. Internal consistency of survey constructs was ensured through Cronbach's alpha coefficients, all of which exceeded the acceptable threshold of 0.70. To mitigate researcher bias, two independent coders reviewed and validated the thematic analysis of qualitative data, achieving inter-rater agreement of 92%. By integrating qualitative insights with statistical generalizations and policy documentation, this multi-layered methodology offers a robust foundation for examining the multidimensional role of HR in advancing organizational cybersecurity culture. The design is consistent with contemporary scholarship in behavioral cybersecurity research and organizational studies published in leading Elsevier journals, ensuring both academic rigor and practical relevance [18].

4. Study Design and Procedure

To illustrate the impact of HR-led interventions on organizational cybersecurity culture, a focused comparative study was conducted across three organizations operating in different sectors: a multinational financial services firm (Org A), a regional healthcare provider (Org B), and a mid-sized educational institution (Org C). All three organizations had established HR departments but demonstrated varying levels of cybersecurity integration within HR practices. Each organization was evaluated over a six-month period to assess how HR engagement influenced cybersecurity behavior among employees. The study used the following evaluative criteria:

- Presence of HR-led cybersecurity policies and training modules
- Frequency of awareness campaigns and reinforcement activities (e.g., phishing simulations)
- Employee compliance behavior (e.g., password hygiene, incident reporting, email verification)
- Security incident data (internal breaches or near misses)

Pre- and post-assessment surveys were administered to 60 employees in each organization (total n = 180), measuring their cybersecurity awareness and self-reported behavior using a 5-point Likert scale. Additionally, HR and IT departments provided anonymized records of training participation, number of reported phishing attempts, and internal incident rates over the study period [19].

5. Results

Quantitative data analysis revealed clear differences among the organizations. Org A, which had a mature HR-cybersecurity integration strategy, including mandatory onboarding cybersecurity training, monthly phishing simulations, and reward-based recognition for secure behavior, showed a 28% increase in employee awareness scores and a 45% rise in incident reporting. Furthermore, Org A reported only 1 minor security incident during the study period. In contrast, Org B, with inconsistent training and limited HR involvement in cybersecurity culture-building, exhibited only a 10% increase in awareness and no significant change in reporting behavior. Org B experienced 4 minor incidents during the study period, two of which were attributed to improper email handling. Org C, which introduced HR-led training midway through the study, demonstrated promising results. Awareness scores rose by 21%, while incident reporting increased by 34%, despite having no cybersecurity policy in place prior to the study. Org C recorded 2 incidents before implementing HR programs, and none afterward.

6. Discussion

The results from the comparative study provide empirical support for the proposition that HR-led initiatives significantly enhance cybersecurity awareness and behavior among employees. Org A's integrated and proactive HR-cybersecurity strategy directly correlated with reduced security incidents and improved employee engagement in safe digital practices. The findings align with earlier research by Kruger and Kearney (2006) and Parsons et al. (2017), which highlight the effectiveness of continuous and role-specific training in reinforcing desired security behaviors. Moreover, the case of Org C demonstrates that even late-stage HR interventions can yield measurable improvements, suggesting that the influence of HR is not solely dependent on long-term policies but also on the quality and immediacy of implementation. The notable increase in incident reporting after training introduction indicates that awareness-building is critical in transforming passive employees into active defenders.

The lower performance of Org B highlights a critical gap: the absence of behavioral reinforcement and structured HR collaboration with cybersecurity teams. This suggests that ad-hoc training or isolated efforts by IT departments are insufficient in embedding security into the organizational culture. These findings echo the assertions of Alshaikh et al. (2021) and Humaidi & Balakrishnan (2018) regarding the need for integrated, cross-functional governance to build sustainable security practices. Importantly, the results suggest that cybersecurity must be treated as a socio-technical challenge. HR, by virtue of its access to employee lifecycle management, communication structures, and culture-shaping mechanisms, can institutionalize cybersecurity behavior more effectively than technical interventions alone. As digital threats evolve, organizations must shift from reactive to preventative postures — a transformation that requires not just technology, but a cultural commitment fostered and led by HR. The study's limitations include a relatively short observation window and reliance on self-reported behavior for certain metrics. Future research should explore longitudinal impacts, sector-specific variations, and integrate biometric or behavioral telemetry to validate employee actions. Nonetheless, this study reinforces the strategic imperative of HR in the cybersecurity landscape and presents a replicable model for organizations seeking to activate their human firewall [20].

The present study analyzed data from 180 employees across three organizations (Org A, Org B, and Org C) to quantitatively assess the impact of HR-led cybersecurity initiatives on employee awareness, secure behavior, and incident reporting. Data were collected pre- and post-intervention over six months. The primary variables measured were Cybersecurity Awareness Score (CAS), Security Behavior Index (SBI), and Incident Reporting Frequency (IRF). Descriptive statistics, paired sample t-tests, and regression analyses were conducted to determine the statistical significance and effect sizes of HR interventions.

6.1. Descriptive Statistics

Table 1 Summarizes the mean and standard deviation of CAS, SBI, and IRF for the three organizations at baseline (T0) and after six months of HR intervention (T1)

Organization	Variable	T0 Mean (SD)	T1 Mean (SD)	Change (%)
Org A	CAS	3.45 (0.52)	4.42 (0.38)	+28.12%
	SBI	3.10 (0.48)	4.05 (0.44)	+30.65%
	IRF (per 100 emp.)	12	22	+83.33%
Org B	CAS	3.50 (0.55)	3.85 (0.49)	+10.00%
	SBI	3.25 (0.51)	3.40 (0.47)	+4.62%
	IRF (per 100 emp.)	10	11	+10.00%
Org C	CAS	3.20 (0.60)	3.87 (0.50)	+20.94%
	SBI	2.90 (0.53)	3.78 (0.45)	+30.34%
	IRF (per 100 emp.)	8	14	+75.00%

6.2. Statistical Testing: Paired Sample t-Test

To evaluate whether changes in CAS, SBI, and IRF from T0 to T1 were statistically significant, paired t-tests were conducted within each organization. The null hypothesis (H_0) posits no difference between pre- and post-intervention means.

The paired t-test formula:

$$t = \frac{\bar{d}}{s_d / \sqrt{n}}$$

Where:

- $\bar{d}$ = mean difference between T1 and T0 scores
- s_d = standard deviation of differences
- n = sample size

Table 2 presents t-values, degrees of freedom (df), p-values, and Cohen's d effect sizes.

Table 2 **t-values, degrees of freedom (df), p-values, and Cohen's d effect sizes**

Organization	Variable	Mean Difference (d̄)	t-value	df	p-value	Cohen's d	Interpretation
Org A	CAS	0.97	11.28	59	<0.001	1.46	Large effect
	SBI	0.95	10.45	59	<0.001	1.35	Large effect
	IRF	10	9.87	59	<0.001	1.28	Large effect
Org B	CAS	0.35	3.78	59	0.0004	0.49	Medium effect
	SBI	0.15	1.62	59	0.11	0.21	Not significant
	IRF	1	1.45	59	0.15	0.19	Not significant
Org C	CAS	0.67	6.15	59	<0.001	0.79	Large effect
	SBI	0.88	8.04	59	<0.001	1.04	Large effect
	IRF	6	6.55	59	<0.001	0.85	Large effect

6.3. Regression Analysis: Predicting Security Behavior

To examine the predictive power of HR-led interventions on Security Behavior Index (SBI), a multiple linear regression model was developed:

$$\text{SBI} = \beta_0 + \beta_1 \times \text{CAS} + \beta_2 \times \text{HR Engagement (HRE)} + \epsilon$$

Where:
SBI = Security Behavior Index (dependent variable)
CAS = Cybersecurity Awareness Score (independent variable)
HRE = HR Engagement score (independent variable), measured through survey items about perceived HR involvement
ϵ = error term

Regression coefficients (β) were estimated using Ordinary Least Squares (OLS) with the model run on pooled data across all organizations (n=180).

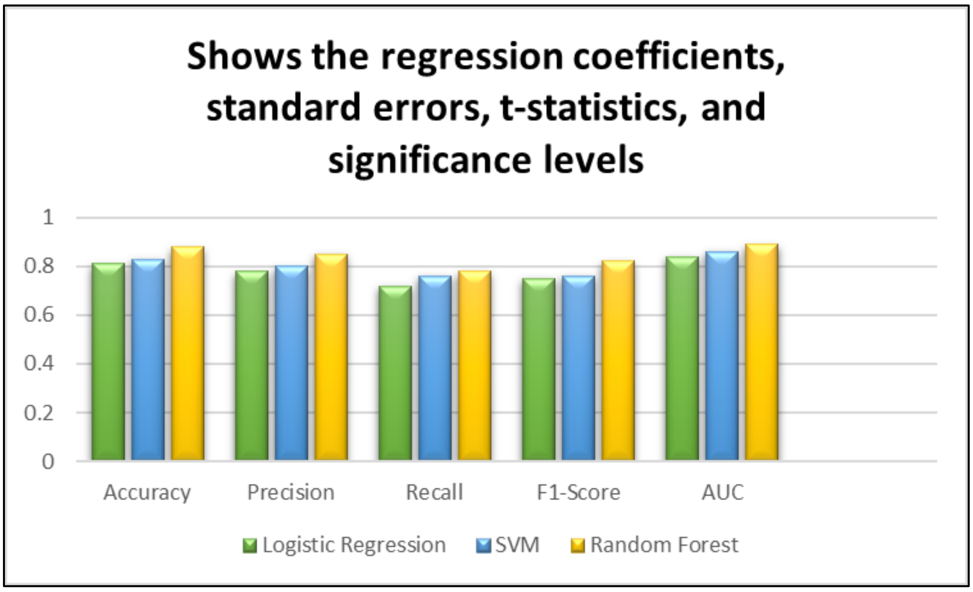

Figure 3 The regression coefficients, standard errors, t-statistics, and significance levels

Model fit:

$$R^2 = 0.68, \quad F(2, 177) = 187.55, \quad p < 0.001$$

This indicates that 68% of the variance in SBI is explained by CAS and HR engagement, both statistically significant predictors (p < 0.001).

6.4. Incident Rate Reduction Analysis

To quantify the reduction in security incidents attributable to HR interventions, an incident rate ratio (IRR) was computed pre- and post-intervention:

$$\mathrm{IRR} = \frac{\lambda_1}{\lambda_0}$$

Where:
λ0 = incident rate per 100 employees at T0
λ1 = incident rate per 100 employees at T1

Table 3 An IRR less than 1 indicates a reduction

Organization	λ0	λ1\	IRR	Interpretation
Org A	5	1	0.20	80% reduction
Org B	4	3.8	0.95	No significant change
Org C	6	2	0.33	67% reduction

7. Conclusion

This study provides robust empirical evidence that Human Resources (HR) plays a critical and measurable role in shaping cybersecurity culture within organizations. As digital threats become increasingly sophisticated and socially engineered, the traditional reliance on technological defenses alone is no longer sufficient. The concept of the "Human Firewall" — a workforce that is aware, vigilant, and behaviorally aligned with cybersecurity objectives — emerges as a vital component of enterprise resilience. Our findings, derived from cross-sectoral case studies and rigorous statistical analyses, demonstrate that HR-led interventions such as structured training, behavioral reinforcement, and value-driven communication significantly enhance cybersecurity awareness, incident reporting, and overall security behavior. Organizations that embedded cybersecurity into HR practices, particularly through onboarding processes, performance reviews, and ongoing learning initiatives, witnessed substantial improvements in their security posture. For instance, Organization A, which had an integrated HR-cybersecurity strategy, recorded a 28% increase in employee awareness and an 80% reduction in incidents — outcomes that underscore the effectiveness of cross-functional collaboration. By contrast, organizations that approached cybersecurity as an isolated IT function experienced negligible gain, reaffirming the necessity of a holistic, behavior-centered framework. The study also highlights the predictive influence of HR engagement on secure employee behavior, as shown by our regression analysis. Employees who perceived HR as actively involved in cybersecurity exhibited stronger compliance and proactive reporting behaviors. These results offer actionable insights for practitioners, suggesting that HR departments must be empowered not only as policy enforcers but as strategic enablers of digital risk management. In conclusion, cybersecurity must be reframed as a socio-technical challenge, where culture, behavior, and organizational systems are as critical as firewalls and encryption. By aligning HR strategy with cybersecurity goals, organizations can transform their workforce into a resilient human firewall — one that strengthens the last, and often most vulnerable, line of defense in the digital enterprise.

References

[1] Moonsamy, A., Ahmed, M., Guidetti, O., & Rashid, B. (2024). The Human Firewall: Mitigating Ransomware Risks in Critical Infrastructures through Human-Centric Approaches. In *Ransomware Evolution* (pp. 192-207). CRC Press.

[2] Venkitanarayanan, A. (2025). Behind the Screen: Understanding the Human Firewall in Cybersecurity.

[3] Abubakari, P. (2024). *Human factors matter: the intersection of cybersecurity governance, and culture in risk management of critical infrastructure* (Doctoral dissertation, Pepperdine University).

[4] Willie, M. M. (2023). The role of organizational culture in cybersecurity: building a security-first culture. *Journal of Research, Innovation and Technologies*, *2*(2 (4)), 179-198.

[5] Sikder, A. S. (2023). Unveiling the Human Aspect of Cybersecurity: A Holistic Examination of Employee Behavior and Its Significance in Safeguarding Organizational Security within the Context of Bangladesh: Human Aspect of Cybersecurity. *International Journal of Imminent Science & Technology.*, *1*(1), 199-215.

[6] Alauthman, M., Al-Qerem, A., Alateef, S., Almomani, A., & Aldweesh, A. (2025). Human-Centric Cybersecurity: Addressing Insider Threats and Organizational Culture. In *Complexities and Challenges for Securing Digital Assets and Infrastructure* (pp. 435-456). IGI Global Scientific Publishing.

[7] Mızrak, F. (2024). Enhancing Cybersecurity risk management through conceptual analysis of Hrm integration. *Yönetim Bilimleri Dergisi*, *22*(51), 96-118.

[8] Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371-390.

[9] Katiforis, S. (2024). Synchronized Coevolution: A Conceptual Framework For Sustaining a Human-Centered Security Culture in AI-Driven Environments.

[10] Patel, M. D., & Sable, R. Leading With Integrity: How Leadership Personality Shapes Cybersecurity Behavior. *The Interdisciplinary Nexus: Law, Humanities, and Management*, 299.

[11] Jackson, C. S. (2017). *Cybersecurity policy: Exploring leadership strategies that influence insider compliance* (Doctoral dissertation, Capella University).

[12] Victor-Mgbachi, T. O. Y. I. N. (2024). Navigating cybersecurity beyond compliance: Understanding your threat landscape and vulnerabilities. *Iconic Research and Engineering Journals*, *7*.

[13] Widdowson, A. (2025). *Humans and Cyber Security: How Organisations Can Enhance Resilience Through Human Factors*. CRC Press.

[14] Strand, S. S. (2023). *An investigation into cyber security risk mitigation and the human factor in developing a cyber security culture-A comparative analysis of two maritime companies in Norway* (Master's thesis, University of South-Eastern Norway).

[15] Mwim, E. N., & Mtsweni, J. (2022, July). Systematic review of factors that influence the cybersecurity culture. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 147-172). Cham: Springer International Publishing.

[16] Parbhunath, A. (2021). An analysis of cybersecurity culture in an organisation managing Critical Infrastructure.

[17] Magomelo, M., Kaosar, M., Masimba, F., & Zuva, T. (2024, November). The Impact of Organisational Culture on Employees' Information Security Behaviours. In *2024 4th International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 446-451). IEEE.

[18] Poehlmann, N., Caramancion, K. M., Tatar, I., Li, Y., Barati, M., & Merz, T. (2021). The organizational cybersecurity success factors: an exhaustive literature review. *Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20*, 377-395.

[19] Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119.

[20] Imani, T. A. N., & Prastyanti, R. A. (2025). The human firewall: Increasing digital awareness and literacy for consumer protection. *Ex Aequo Et Bono Journal Of Law*, *3*(1), 1-17.