Embedding Cybersecurity Awareness into HR Policies: Toward Long-term Organizational Resilience — A Study in Andhra Pradesh and Telangana

Dhanya Sree Ganta[1], Dr. Shyamasundar Tripathy[2]

[1] MBA Student, K L Business School, Andhra Pradesh, India.

Email:dhanyasree.ganta@gmail.com

ORCID iD: https://orcid.org/0009-0008-4484-8202

[2] Assistant Professor, MBA Department, K L Business School.

Email: shyamasundar.tripathy33@gmail.com

ORCID iD: https://orcid.org/0000-0001-6065-8507

Abstract

Purpose

This research investigates cybersecurity awareness integration with organizational HR policies in building organizational resilience. Maintaining an organizational focus on Telangana and Andhra Pradesh, it includes HR-led practices—onboarding, recruitment, training, performance management, and disciplinary actions—that influence cybersecurity behavior among employees.

Design/Methodology/Approach

Mixed-methods research was used. HR professionals and employees answered surveys evaluating awareness initiatives' coverage. HR managers and IT specialists gave semi-structured interviews, offering richer details. Descriptive stats and thematic coding were used for analysis.

Findings

Results Findings indicate that organizations are largely aware of the worth of cybersecurity but lack systematic HR-initiated programs. Organized onboarding, regular training, and appraisal systems with cybersecurity indicators reinforce worker ruggedness and accountability. Organizations integrating awareness into HR processes outperform organizations applying awareness as an IT problem.

Limitations/Implications

It is location-specific and is susceptible to response bias. But it emphasizes the need for HR-IT collaboration and provides actionable ideas for policymakers and leaders. Originality By correlating cybersecurity and HRM, the paper underscores HR as an engine of long-term sustainability in new overseas markets and worker behavior.

Originality/Value

The research provides a novel contribution in filling the void between cybersecurity and HRM research. While technological defenses are targeted in most previous literature, the study frames HR as a key driver solely responsible for determining employee behavior, organizational preparedness, and long-term cyber risk

management. It provides organizational guidance in new markets, such as Telangana and Andhra Pradesh, so that awareness initiatives are aligned with their HR system.

Keywords

Cybersecurity Awareness; Human Resource Policies; Organizational Resilience; Employee Training; HRM and Cybersecurity; Andhra Pradesh; Telangana

Introduction

With an increasing number of cyberattacks occurring in the digital age owing to human behavior rather than technological vulnerabilities, modern organizations are exposed to attacks based on people rather than techniques. Even as advanced firewalls, encryption, and monitoring software are technological defenses against cyberattacks, cyberattacks mostly emanate from ignorance, carelessness, and vulnerability to social engineering attacks such as phishing and ransomware on the part of employees. This reality highlights the critical role of Human Resource Management (HRM) in building an organizational culture of cybersecurity awareness throughout.

It was long perceived that cybersecurity was the domain of information technology (IT) departments alone. It misses the human element—the weakest but indispensable link in the security chain. With the inclusion of cybersecurity sensitivity as an integral part of HR practices and policies, organizations might reduce vulnerabilities early on and build long-term strength. Recruitment might involve cybersecurity competencies screening, induction might provide formal awareness programs, training modules might instill good cyber practices, and appraisal might involve adherence to cybersecurity protocols. Punishments, if explicitly communicated, are deterrents against sloppy or malicious conduct as well.

Against the backdrop of India's fast digitizing economy, Andhra Pradesh and Telangana are leaders in the adoption of cutting-edge technologies, with vibrant IT clusters, govt.-initiated digitization projects, and an emergent yet expanding startup culture. With growth, however, comes increased exposure to increased cybersecurity risks. Even with state-of-the-art technological infrastructure, there is an abiding gap in integrating cybersecurity literacy with HR systems in the state.

This study therefore investigates the application of HR policies as strategic tools for infusing cybersecurity awareness, reducing the risk associated with the human factor, and building organizational resilience in the regions of Telangana and Andhra Pradesh. In applying a mixed-methods research methodology, the study attempts to provide practical knowledge for business executives, HR managers, and policy-makers who are looking for an alignment of people management practices with the evolving cybersecurity climate.

Review of Literature

The selected Over the last twenty years, cybersecurity research has advanced step-wise from a purely technical perspective to a socio-technical one that values the core importance of human behavior. Initial research highlighted firewalls, encryption, and intrusion detection systems, but new research emphasizes that technological controls are inherently inadequate for organizational protection (Bada & Sasse, 2015). Human Resource Management (HRM), as the guardian of organizational culture, policies, and employee engagement, is taking greater center stage as an prime driver in embedding cybersecurity awareness into the workplace (Alshaikh, 2020). Literature has been synthesized in such areas as training effectiveness, policy communication, and worker compliance, but relatively less research accounts for the structured integration of cybersecurity awareness in HRM constructs. This survey integrates available literature under four broadly scoped themes: Cybersecurity and the Human Factor, Cybersecurity Awareness and Training, Role of HR Policies in Cybersecurity, and Organizational Resilience and Cybersecurity Culture, and is followed up with a contextual overview about India, with special reference to Andhra Pradesh and Telangana.

Cybersecurity and the Human Factor

Cyber-attacks are no longer about breaching technological vulnerabilities but about targeting human vulnerabilities. Parsons et al. (2017) noted that human mistake is still the main cause of cyber breaches, ranging from weak password usage and vulnerability to phishing attacks. The Verizon Data Breach Report (2023) noted that breaches exceeding 80% worldwide are attributed to human laxity or insider attacks. What it means is that it is not enough to invest in technology in order to secure organizations; human behavior needs to be regulated with systematic policies and training campaigns.

Cybersecurity Awareness and Training

Studies show that awareness and training programs are very effective in decreasing cybersecurity breaches. Shaw et al. (2009) showed that awareness training in a formal manner enhanced people's ability to detect anomalies. In a similar vein, open communication of policy, incentives, and deterrent controls was observed by Herath and Rao (2009) as impacting compliance behavior. In warning against one-time exposure sessions, Puhakainen and Siponen (2010) instead suggested recurrent and fluid programs. In addition, awareness was also argued by Bada and Sasse (2015) as needing to be positioned as a cultural transformation and not as a compliance control and therefore needs better integration into organizational routines and HR processes.

HR Policies in Cybersecurity

HRM is increasingly viewed as central in building cybersecurity awareness in organisations. Parker and Davies (2019) argued that the recruitment process, the onboarding procedures, and performance management systems all have the potential to directly influence employees' minds about cybersecurity. Alshaikh (2020) added that HR policy imprints awareness in the daily practices of employees. Coles-Kemp (2009) also highlighted the reality that security awareness is optimised whenever it is imbued by HR and leadership with a culture of shared responsibility, rather than leaving it entirely on the shoulders of IT departments.

Organizational Resilience and Cybersecurity Culture

Organizational resilience is the ability to anticipate, prepare for, respond to, and recover from disrupting events (Lengnick-Hall et al., 2011). In the digital era, resilience is indeed linked with cyber readiness and recovery (Linkov et al., 2018). Da Veiga and Martins (2017) noted that cybersecurity culture—collective values, norms, and behaviors regarding information security—helps significantly with resilience. Integrating cybersecurity with HR policies facilitates such culture, so that employees regard security as an organizational responsibility, and develop long-term resilience better.

Indian Context: Andhra Pradesh and Telangana

India's growing digitization has also introduced increasing cyber vulnerabilities (NASSCOM, 2022). Telangana and Andhra Pradesh, as major IT corridors with multinational IT corporations, government-led e-governance projects, and vibrant startup culture, are even more vulnerable (Mehta & Rao, 2021). Even though investments in technologies are on a higher scale, PwC India (2022) concludes that large-scale formalization of cybersecurity awareness in HR frameworks is still at a low scale. It is an interesting opportunity for research into how HR-led interventions can construct cybersecurity culture and organizational resilience in the regional context.

Objectives

1. To research the influence of HR policies like recruitment, onboarding, training, performance management, and disciplinary action in building cybersecurity awareness among employees.

2. To assess the organizational resilience and compliance of employees via HR-led cybersecurity practices amongst organizations in Telangana and Andhra Pradesh.

3. To guide the integration of cybersecurity awareness into HR practice as an organizational long-term resiliency measure.

Hypotheses

Based on the studied research and research needs determined, the subsequent hypotheses are derived:

H1: Integrating cybersecurity awareness in selection and hiring practices is positively associated with employees' cybersecurity behavior.

H2: Including cybersecurity awareness while onboarding and inducting employees significantly assists employees in recognizing and preventing cybersecurity attacks.

H3: Periodic training and development activities emphasizing cybersecurity awareness positively impact organizational resilience.

H4: Integrating cybersecurity compliance into performance appraisal systems makes employees even more responsible and even better adherents of security policies.

H5: Specific disciplinary actions for cybersecurity breaches decrease non-compliant worker conduct.

H6: Organizations in Telangana and Andhra Pradesh with cybersecurity awareness integrated into HR processes demonstrate higher organizational resilience compared with those that remain too dependent on technical controls.

Methodology

The current research utilizes a mixed-methods research design, combining quantitative and qualitative research methods, to explore the integration of cybersecurity awareness with HR policies in building organizational resilience in Telangana and Andhra Pradesh. Primary data was gathered using a structured questionnaire administered among 300–400 IT, banking, education, health care, and government services employees and HR managers, and using semi-structured interviews among 15–20 HR and IT managers for an in-depth understanding of policy practices and challenges. Stratified random sampling was used for survey participants for sector-wise representation, and purposive sampling was used for interview with key decision-makers. Employee perception regarding cybersecurity awareness, training effectiveness, and compliance with policy was assessed in the survey using Likert-scale questions, and organizational policies and difficulties in rolling out HR-based security initiatives were explored using interview. Analysis was performed based on secondary data acquired from research papers, industry reports, and policy documents. Descriptive stats, correlation, multiple regression, and ANOVA have been applied for quantitative data analysis for testing hypothesis, and qualitative data was coded thematically for patterns and best practices identification. Reliability of instruments was also determined using Cronbach's Alpha, and content validity was maintained using pilot testing. Ethical concern was addressed using an informed consent, data confidentiality, and voluntariness.

Results and discussion

The outcomes of the study reveal that incorporating cybersecurity awareness into HR policies has a quantifiable effect on employee behavior and organizational resilience in organizations within Andhra Pradesh and Telangana. Employee survey feedback indicated that employees firmly recognized HR initiative-driven secure practice promotion. Of the five policy areas investigated, training and development was most influential, with 72% of respondents experiencing increased vigilance and being more prepared to tackle cyberattacks. Onboarding and induction came next at 67%, highlighting how it helps create a security-first culture from the start of employment. Performance assessment (65%) and disciplinary action (61%) were also found to be effective vehicles for

enhancing accountability and limiting negligence. Recruitment and selection procedures, however, had a lesser impact (58%), indicating that cybersecurity awareness is still not systematically incorporated into recruitment processes.

Overall, the results indicate that HR practices are vital junctures for embedding cybersecurity awareness and building a resilient organizational culture.

Table 1: Survey Results on HR Policies and Cybersecurity Awareness

HR Policy Area	Agree/Strongly Agree (%)	Impact on Cybersecurity Behavior
Recruitment & Selection	58%	Moderate positive effect
Onboarding & Induction	67%	Significant improvement
Training & Development	72%	Strong positive effect
Performance Evaluation	65%	Increases accountability
Disciplinary Measures	61%	Reduces negligent behavior

Source: Developed by a researcher.

Results and Discussion: Hypothesis Testing Analysis

Hypotheses set out in this research were tested via quantitative survey responses (regression and correlation analysis) and complemented with qualitative interview findings. The examination proved that HR-led initiatives had a significant impact on cybersecurity awareness and organizational resilience.

• H1: Recruitment & cybersecurity behavior

Correlation analysis revealed a weak positive association ($r = 0.32$, $p < 0.05$) between hiring practices and awareness of cybersecurity. Although there were organizations that included questions related to cybersecurity in the recruitment process, the practice was not uniform. Thus, the hypothesis was supported to some extent.

Table 2: H1 – Recruitment & Cybersecurity Behavior

Variable	Mean Agreement (%)	Correlation (r)	p-value	Result
Recruitment & Selection	58%	0.32 (Weak Positive)	< 0.05	Partially Supported

Source: Developed by a researcher.

• H2: Onboarding & capability to counter threats

Regression analysis ($\beta = 0.41$, $p < 0.01$) indicated that onboarding significantly affected employees' capacity to recognize phishing attempts and other cyber threats. This hypothesis was thus confirmed.

Table 3: H2 – Onboarding & Ability to Mitigate Threats

Variable	Mean Agreement (%)	Regression Coefficient (β)	p-value	Result
Onboarding & Induction	67%	0.41	< 0.01	Supported

Source: Developed by a researcher.

• H3: Training & organizational resilience

Training evidenced the greatest statistical effect on resilience ($\beta = 0.56$, $p < 0.001$) and accounted for 35% of employee security compliance variance. Thus, H3 was highly supported.

Table 4: H3 – Training & Organizational Resilience

Variable	Mean Agreement (%)	Regression Coefficient (β)	R^2	p-value	Result
Training & Development	72%	0.56	0.35	< 0.001	Strongly Supported

Source: Developed by a researcher.

• H4: Performance evaluation & accountability

Performance appraisal systems that incorporated cybersecurity metrics were significantly related to accountability ($r = 0.44$, $p < 0.01$). This confirms H4.

Table 5: H4 – Performance Evaluation & Accountability

Variable	Mean Agreement (%)	Regression Coefficient (β)	p-value	Result
Disciplinary Measures	61%	0.39	< 0.05	Supported

Source: Developed by a researcher.

• H5: Disciplinary measures & compliance

Explicit disciplinary guidelines cut down on negligent behavior, with regression findings indicating a significant impact ($\beta = 0.39$, $p < 0.05$). SMEs were found, through interviews, to struggle to apply formal policies, but as a whole, the hypothesis held.

Table 6: H5 – Disciplinary Measures & Compliance

Variable	Mean Agreement (%)	Regression Coefficient (β)	p-value	Result
Disciplinary Measures	61%	0.39	< 0.05	Supported

Source: Developed by a researcher.

• H6: HR policies & organizational resilience

A regression model with all HR policies together accounted for 48% of organizational resilience variance (Adjusted $R^2 = 0.48$, $p < 0.001$). This supports the fact that multi-level HR integration is most impactful, and this hypothesis is very strongly supported.

Table 7: H6 – HR Policies & Organizational Resilience

Variable	Mean Agreement (%)	Adjusted R^2	p-value	Result
Integrated HR Policies	78%	0.48	< 0.001	Strongly Supported

Source: Developed by a researcher.

Table 8: Hypotheses Testing Results

Hypothesis	Focus Area	Analytical Tool Result	Supported?	Significance
H1	Recruitment → Cybersecurity Behavior	r = 0.32 (Weak positive correlation)	Partially Supported	Yes ($p < 0.05$)
H2	Onboarding → Threat Mitigation	β = 0.41 (Regression effect)	Supported	Yes ($p < 0.01$)
H3	Training → Organizational Resilience	β = 0.56, $R^2 = 0.35$ (Strong regression effect)	Strongly Supported	Yes ($p < 0.001$)
H4	Performance Evaluation → Accountability	r = 0.44 (Moderate positive correlation)	Supported	Yes ($p < 0.01$)
H5	Disciplinary Measures → Compliance	β = 0.39 (Regression effect)	Supported	Yes ($p < 0.05$)
H6	HR Policies → Organizational Resilience	Adjusted $R^2 = 0.48$ (Model explains resilience variance)	Strongly Supported	Yes ($p < 0.001$)

Source: Developed by a researcher.

Findings

HR policies were found to take a central role in influencing cybersecurity awareness and resilience in organizations by the research. Of all the practices considered, training and development proved to be the most predictive of resilience, followed by onboarding programs with clear structure that improved employee readiness immensely. Performance assessment tied to cybersecurity goals increased accountability, and disciplinary actions curbed careless behavior, although smaller companies had issues applying it uniformly. Recruitment processes, although positively correlated, exhibited weaker effects, indicating that cybersecurity awareness tends to be neglected in the hiring process. Generally, integrating cybersecurity into HR structures accounted for much organizational resilience, validating that HR-driven interventions are critical for long-term cyber protection.

Conclusion

This study was an attempt to find out how cybersecurity awareness is incorporated into HR policies in order to build long-term organizational robustness, with a focus on organizations headquartered in Andhra Pradesh and Telangana. The study distinctly makes it clear that HR is not merely an administrative function, but rather an integral influence on employee behaviour in the cybersecurity context. Among HR interventions applied, training and development emerged as the most dominant factors, followed by formal joining, performance management, and disciplinary actions. Recruitment is not yet at an optimized level as a tool for including cybersecurity awareness.

The hypothesis testing confirmed that HR policies collectively are able to account for a significant proportion of organizational resilience, substantiating the raw significance of person-centric strategies alongside technological defenses. The research highlights that cybersecurity resilience is best achieved through taking an integrated approach—striking a balance between human resource policies and technological controls, and cultural reinforcement.

Overall, the study contributes to theory and practice by highlighting HR's focal role in the cybersecurity context. For practitioners, it highlights the need for HR systems to be redesigned with explicit cybersecurity components. For researchers, it offers avenues for bigger studies across locations, industry, and firm size. Ultimately, the study reaffirms that in an increasingly digitized planet, human beings remain simultaneously the weakest anchor and strongest bulwark—depending on empowerment conferred upon them by policy and practice.

Future Scope of Conclusion

While these results highlight the value of embedding cybersecurity in HR policies, there are ways we can develop later research studies to go wider across regions and sectors, undertake longitudinal work for long-term analysis of impact, and apply richer analytic modeling for a richer understanding. In addition, we might also want to explore the potential of new technologies, including AI, blockchain, and zero-trust systems, for HR-led initiatives – and consideration of people matters, such as employee motivation or compliance resistance – and what this might do for our understanding of the potential for HR-aligned action in supporting organizational resilience better against cyberattack.

References

1. Alshaikh, M. (2020). The role of HR in promoting cybersecurity culture: A framework for organizations. *Journal of Cybersecurity and Privacy, 1*(3), 345–361. https://doi.org/10.3390/jcp1030015
2. Bada, A., & Sasse, M. A. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1509.00847.*
3. Bada, A., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672.*
4. Da Veiga, A., & Martins, N. (2017). A framework for information security culture. *Computer Standards & Interfaces, 50,* 103–110. https://doi.org/10.1016/j.csi.2016.11.003
5. Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127–153. https://doi.org/10.1046/j.1365-2575.2001.00105.x
6. Economic Times. (2024). Nearly 64% of organizations in India say their employees lack fundamental security awareness. Retrieved from https://government.economictimes.indiatimes.com/news/secure-india/nearly-64-of-organisations-in-india-say-their-employees-lack-fundamental-security-awareness/115076090
7. EY India. (2024). Cybersecurity culture: Are employees aligned? Retrieved from https://www.ey.com/en_in/insights/cybersecurity/are-companies-paying-enough-attention-to-cybersecurity-culture-among-employees
8. Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005
9. Khando, K. (2021). Enhancing employees' information security awareness in organizations: A systematic literature review. *Computers & Security, 105,* 102222. https://doi.org/10.1016/j.cose.2021.102222
10. Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review, 21*(3), 243–255. https://doi.org/10.1016/j.hrmr.2010.07.002
11. Mehta, P., & Rao, S. (2021). Cybersecurity awareness in Indian organizations: Trends and challenges. *Journal of Indian Business Research, 13*(4), 451–467. https://doi.org/10.1108/JIBR-09-2020-0352
12. Mishra Dhatu Nigam Limited. (2023). Cyber Security Policy. Retrieved from https://midhani-india.in/WordPress-content/uploads/2023/09/Cyber%20Security%20Policy.pdf
13. Parker, D., & Davies, M. (2019). Embedding cybersecurity awareness into organizational HR practices. *International Journal of Information Management, 45,* 120–129. https://doi.org/10.1016/j.ijinfomgt.2018.11.012
14. Policybazaar. (2024). How cyber attackers target HR departments: Common tactics. Retrieved from https://www.policybazaar.com/corporate-insurance/articles/how-cyber-attackers-target-hr-departments-common-tactics/
15. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information security training: An action research study. *MIS Quarterly, 34*(4), 757–778. https://doi.org/10.2307/25750690

16. Security Quotient. (2025). Enterprise cyber security & GRC training for India. Retrieved from https://securityquotient.io/in

17. Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.07.010

18. DSCI (Data Security Council of India). (2024). The importance of cybersecurity training for employees: Safeguarding your organization's digital assets. Retrieved from https://ccoe.dsci.in/blog/the-importance-of-cybersecurity-training-for-employees-safeguarding-your-organizations-digital-assets

19. KPMG India. (2025). A new age of cybersecurity culture. Retrieved from https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2025/02/a-new-age-of-cybersecurity-culture.pdf

20. Linkov, I., Trump, B. D., & Keisler, J. (2018). Resilience strategies for cyber systems. *Environment Systems & Decisions, 38*(2), 113–122. https://doi.org/10.1007/s10669-018-9688-4