WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Study on Data Ethics and Cybersecurity in Human Resource Management in IT Sector, in Bengaluru

Sneha.V[1] , Preethi.B[2] , Dr. Veena Bhavikatti[3]

[1,2] Department of MBA, AMC Engineering College, Bangalore-560083
[3]Associate Professor, Department of MBA, AMC Engineering College, Bangalore 560083

ABSTRACT:

In today's fast-paced digital world, Human Resource Management (HRM) is no longer just about hiring and onboarding it's also about protecting the digital footprints of employees. This project explores the rising importance of data ethics and cybersecurity in HR practices within the IT sector, where sensitive employee information is stored, analyzed, and sometimes even interpreted by AI-powered systems. As HR departments increasingly adopt digital tools from cloud-based HR platforms to AI-driven recruitment algorithms new ethical and legal challenges emerge. This research combines primary data (surveys and interviews with HR professionals) and secondary data (existing literature, regulations like GDPR, HIPAA, and India's DPDP Act) to uncover how HR teams manage the delicate balance between compliance, technology, and human trust. Findings reveal that while awareness of data protection is growing, gaps still exist in training, policy enforcement, and ethical decision-making especially in remote and AI-enhanced work environments. The study concludes that for the IT sector, it's no longer enough for HR to be people-focused; it must also be data-responsible. Meaningful change will require a cultural shift where cybersecurity and ethics are not just checkboxes, but core values of the modern HR function.

KEY WORDS: *Data Ethics in HR, Cybersecurity in Human Resource Management, AI and Automation in HR Decisions, Employee Data Privacy, Legal Compliance (GDPR, HIPAA, DPDP).*

INTRODUCTION:

In today's digital age, human resource management in the IT sector has transformed significantly. With the rise of advanced technologies, HR professionals are no longer just managing resumes and interviews they're handling vast amounts of sensitive employee data: personal details, financial information, health records, and performance metrics. With this shift comes a new and critical responsibility: ensuring data ethics and cybersecurity.

Data ethics refers to the responsible use, collection, and handling of data. In HR, this means treating employee data not just as a resource, but as a reflection of real people with rights and expectations of privacy. Ethical data practices ensure that information is used transparently, fairly, and only for appropriate purposes. For example, if an HR system uses AI to screen candidates, it's essential to make sure it doesn't reinforce bias or discrimination.

RESEARCH QUESTIONS:

1. How well are HR professionals in the IT sector equipped to handle ethical challenges related to employee data privacy and cybersecurity?
2. What are the biggest obstacles HR departments face in implementing data privacy and cybersecurity policies in IT companies, and how do they overcome them?
3. In what ways does employee awareness of data ethics influence the effectiveness of cybersecurity practices in HR within IT organizations?
4. How do IT sector companies ensure ethical transparency in the use of AI and surveillance technologies during recruitment, performance monitoring, or remote work?
5. To what extent does regular cybersecurity training for HR staff in the IT industry improve compliance with global data protection laws like GDPR or CCPA?

RESEARCH OBJECTIVES:

- To explore how HR teams in IT companies are currently handling sensitive employee data and whether they are aware of the ethical and legal responsibilities that come with it.

- To understand the cybersecurity risks HR professionals face in today's digital-first and remote-friendly workplace, especially when using platforms that store or analyze personal data.
- To investigate how new technologies like AI, cloud-based systems, and employee monitoring tools are changing the ethical landscape of HR management in IT firms.
- To identify practical, real-world strategies that HR teams can adopt to strengthen cybersecurity while still respecting employee privacy and trust.
- To recommend policy or training improvements that help bridge the gap between legal compliance, ethical practice, and day-to-day HR operations in the IT industry.

REVIEW OF LITERATURE:

Isabel Ebert (2021), Privacy Due Diligence as a Human Rights-Based Approach to Employee Privacy Protection, Ebert proposes a human rights-centered privacy model. Her work critiques technical/legal fixes and introduces a privacy due diligence approach emphasizing employee agency and responsibility in the face of surveillance and algorithmic management in the digital workplace.

Denita Kozhuharova (2022), Ethics in Cybersecurity: What Are the Challenges We Need to Be Aware Of and How to Handle Team, Kozhuharova stresses the ethical foundations in cybersecurity, especially in research and product development. Citing EU's GUARD project, she outlines challenges like privacy, incidental findings, and bias. She proposes a cross-disciplinary ethical methodology for technology and HR alignment.

Ramesh Nyathani (2023), Safeguarding Employee Data: A Comprehensive Guide to Ensuring Data Privacy in HR Technologies, Nyathani offers a practical guide for HR on protecting digital employee data. He identifies current risks like third-party breaches and emphasizes building a culture of privacy through compliance, employee awareness, and tech safeguards within HR tech platforms.

Hani Zaki (2024), The Influence of Cybersecurity on Human Resources Legal Practices and Ethical Standards, Zaki explores how the growing integration of cybersecurity in HR reshapes legal responsibilities and ethical standards. HR must now align with laws like GDPR and CCPA while maintaining employee data privacy and transparency. The study highlights the shift towards proactive training, ethical data usage, and the challenge of managing remote work securely.

Naida Junaid (2024), Legal Compliance and Ethical Challenges in Cybersecurity for Human Resources Management, Junaid addresses the dual challenge HR faces in complying with data regulations and maintaining ethical integrity. As remote work and BYOD become more common, HR must evolve secure, adaptable systems while balancing organizational needs with employee privacy through education and policy development.

Sanket Ramakant Lodha (2024), Data Privacy and Security in HR Systems, Lodha focuses on the integration of IoT in HR and its associated risks. He introduces a framework for HR to navigate privacy and security challenges, especially within Industry 4.0, and stresses strategic involvement in tech decisions.

Zaheer Abbas (2024), Cybersecurity Protocols in Human Resources: Ensuring Legal Compliance and Ethical Standards, Abbas discusses how HR can build cybersecurity resilience through continuous training and collaboration with IT. He includes case studies and outlines ethical best practices for managing sensitive employee data within legal frameworks.

Tariq Jameel (2024), Cybersecurity Knowledge Among HR Employees: Effects on HR Laws and Practices, Jameel connects HR's cybersecurity literacy with effective law enforcement in data protection. Survey-based findings show critical knowledge gaps, prompting the need for focused training programs in HR departments.

Wasif Ali & Leonidas Gulbas (2024), Human Resources Compliance with Cybersecurity Principles: Legal and Ethical Dimensions, This paper highlights the importance of balancing security measures with employee rights. It recommends collaboration across HR, IT, and legal teams to build transparent, ethical data access and monitoring systems.

Prabhu Manoharan (2024), A Review on Cybersecurity in HR Systems: Protecting Employee Data in the Age of AI, Manoharan examines how AI boosts cybersecurity in HR but also introduces new challenges like algorithmic bias. He calls for adaptive systems and ethical oversight in deploying AI tools to safeguard employee information.

Asif Ali & Sebastian Thrun (2024), Human Resources Laws and Cybersecurity Principles: Ensuring Compliance and Ethical Standards, Ali and Thrun advocate for integrating cybersecurity into HR legal frameworks. They suggest applying access controls, regular audits, and employee training to protect rights and maintain trust in data governance.

Leonidas Guibas (2024), Human Resources Compliance with Cybersecurity Principles: Legal and Ethical Dimensions, Echoing his co-authored work, Guibas reinforces the need for balanced HR practices. He promotes forming strong internal policies and building a privacy-respecting culture through continuous education and cross-functional teamwork.

Steven Robbins (2024), Legal and Ethical Aspects of Cybersecurity Integration in Human Resources Management, Robbins explores the tension between enforcing cybersecurity and upholding employee rights. He advocates for transparency, consent-based monitoring, and ethical use of surveillance tools within legal limits.

Amina Malik (2024), The Ethical Implications of Big Data in Human Resource Management, Malik warns against the misuse of big data in HR for profiling and control. She encourages HR to adopt moral principles when deploying data analytics to ensure fairness across recruitment, evaluation, and compensation processes.

Sagar Ali & Judea Pearl (2024), Cybersecurity Principles in HRM: Compliance with Legal Framework and Ethical Consideration, Ali and Pearl present best practices for HR cybersecurity, integrating legal and ethical perspectives. They promote regular audits, adoption of advanced tech, and widespread staff training to create a secure HR environment.

RESEARCH GAP:

Table 1: Review analysis:

S. No	Citations & year	Research design	Objectives	Findings
1	Isabel Ebert(2021)	Methodological proposal	Present a human rights approach to employee privacy.	Privacy Due Diligence strengthens ethical accountability.
2	Denita Kozhuharova(2022)	Case analysis	Address ethical concerns in cybersecurity technology.	Proposes a methodology blending ethics and cybersecurity.
3	Ramesh Nyathani(2023)	Review Analysis	Provide a practical guide for HR data privacy	Risks include unauthorized access and third-party breaches.
4	Hani zaki (2024)	Descriptive review	Analyze the impact on remote work management	Cybersecurity enhances compliances with laws like GDPR and CCPA.
5	Naida Junaid (2024)	Theoretical analysis	Assess legal and ethical issues in HR cybersecurity	Balancing data use and privacy is a major ethical challenges.
6	Sanket Ramakant Lodha(2024)	Systematic Review analysis	Explore security and privacy challenges from IoT in HR.	HR must evolve strategically to partner with technology.
7	Zaheer abbas(2024)	Case study-based analysis	Examine the interplay of legal, ethical, and cybersecurity in HR.	Trust, transparency, and fairness are ethical imperatives.
8	Tariq Jameel(2024)	Empirical study (based on survey)	Investigate HR staff knowledge of cybersecurity.	Enhanced knowledge boosts HR's data protection role.
9	Wasif Ali, et al (2024)	Conceptual paper	Promote training and policy development.	Collaborative HR-IT efforts improve organizational cybersecurity.
10	Prabhu Manoharan (2024)	Critical literature review	Identify threats and AI-enabled defenses.	Dynamic protocols and regulatory updates are needed.
11	Asif Ali, et al (2024)	Conceptual analysis	Bridge HR legal frameworks with cybersecurity best practices.	Best practices include encryption, audits, and employee education.
12	Leonidas Guibas(2024)	Conceptual analysis	Examine cybersecurity's legal and ethical implications in HR.	Ethical practices involve non-biased monitoring and training.
13	Steven Robbins(2024)	Analytical discussion	Explore how integrating cybersecurity affects HR law and ethics.	Balancing data security with employee privacy is critical.
14	Amina Malik(2024)	Ethical theoretical analysis	Explore ethical concerns in using big data across HR functions.	Big Data Analytics may conflict with ethical HR values.

15	Sagar Ali, et al,(2024)	Review analysis	Integrate cybersecurity into HR to meet legal and ethical obligations.	Legal compliance and ethics both demand robust protection.

CONCEPTIONAL MODEL:

Fig. No. 1 conceptional model of data ethics and cybersecurity in human resource management in IT sector

PROBLEM STATEMENT:

In today's digital-first workplace, especially within the fast-paced IT sector, Human Resource Management (HRM) plays a critical role not only in managing people but also in safeguarding their most sensitive data. From recruitment to retirement, HR departments handle large volumes of personal and confidential information like ID proofs, bank details, health records, and performance reviews. As IT companies embrace AI-driven HR tools, cloud platforms, and data analytics to enhance productivity, a growing concern has emerged around data ethics and cybersecurity.

- Low awareness of data ethics among HR professionals.
- Inadequate cybersecurity measures in HR systems.
- Employee concerns about misuse of personal data.
- Lack of transparent data privacy policies.
- Over-reliance on AI in HR without ethical oversight.
- Minimal employee involvement in data governance.
- Ethical compliance is often ignored during digital transformation.
- Limited or no incident response plans for data breaches in HR.
- Inconsistent cybersecurity practices between HR and IT departments.
- Employees fear retaliation for reporting data misuse or ethical concerns.

This research addresses this pressing problem by exploring how HR departments in IT companies can align ethical data practices with robust cybersecurity frameworks. It seeks to understand current practices, awareness levels, and policy gaps while emphasizing the need for ethical leadership, transparent policies, and employee empowerment in data governance.

RESEARCH METHODOLOY:

METHODS:

Survey Method:

Structured questionnaires shared with HR professionals and IT employees. Focused on collecting data about awareness, practices, and concerns on data ethics and cybersecurity.

Primary Data:

Structured questionnaire distributed via Google Forms or email.

Semi-structured interviews with selected HR leaders and cybersecurity experts to gather deeper ethical perspectives.

Secondary Data:

Journals, case studies, industry reports, and company policies on HR data management and cybersecurity.

VARIABLE DESCRIPTION:

Table 2: variable description on data ethics and cybersecurity in human resource management in IT sector.

Variable	Type	Description
Name/Email	Demographic	Personal identifier (used only for data matching and privacy-compliant segmentation).
Age Group	Demographic	Respondent's age range — helps analyze cybersecurity awareness by generation.
Educational Qualification	Demographic	Level of education — useful to assess understanding of data security principles.
Gender	Demographic	Gender identity helps assess inclusiveness in HR and security training outreach.
Location	Demographic	Geographical region used to compare regional trends in HR ethics and cybersecurity.
Awareness of HR policies	Independent Variable	Measures how well the employee knows HR policies, impacting cybersecurity behavior.
Company Ensures Data Security	Independent Variable	Indicates whether the company has protective data security mechanisms in place.
Consent to Data Use	Independent Variable	If the employee gives informed consent to how their data is used core ethical metric.
Additional Comments on Ethics	Qualitative	Open-ended views used for qualitative sentiment analysis or coding.
Transparency of Data Handling	Independent Variable	Perceived transparency in how HR handles personal data a key ethical driver.
Satisfaction with HR Practices	Dependent Variable	How respondents rate HR's performance in secure, ethical handling of data.
Employee Participation in Policy	Independent Variable	If employees are actively engaged in cybersecurity and HR policy-making.
Awareness of Security Threats	Dependent Variable	Whether the respondent is familiar with cyber threats like phishing, ransomware, etc.
Cyber Threat Types Identified	Dependent Variable	Types of cyber threats reported by respondents shows awareness level.
Suggestions for HR Improvement	Qualitative	Respondents' recommendations for improving HR cybersecurity and ethics used for thematic analysis.

Target Population:

HR professionals, IT managers, and employees working in mid-to-large-scale IT companies.

Sampling Method:

For this survey, we used a simple and practical way to gather responses we reached out to people who were easy to contact and willing to participate. This included HR professionals and employees working in IT companies, mainly in mid-sized firms. Most of the responses were collected through online surveys, like Google Forms, which made it quicker and easier to get feedback. This method is called convenience sampling, and while it helped us collect

useful insights in a short time, it might not fully represent everyone working in the IT sector. Still, it gave us a good starting point to understand what people think and experience when it comes to data ethics and cybersecurity in HR.

SAMPLE SIZE:

51 respondents received, including both HR personnel and employees from IT departments across various companies.

Sample size ensures coverage across sectors and zones and allows reliable statistical analysis at 95% confidence level.

ANALYSIS AND DISCUSSION:

The survey collected response from 51 fresh employees including HR professionals and managers working in the mid-sized IT companies. The survey, designed to explore the intersection of data ethics, cybersecurity, and HR practices in the IT sector, reveals a blend of progress, awareness, and noticeable gaps across organizations. Here's a detailed interpretation of the responses:

- **Demographic Profile of Respondents**

Age Group Distribution:

AGE GROUP	APPROXIMATE COUNT	PERCENTAGE
Under 18	0	0%
18-25	27	53%
25-35	12	23.5%
36-50	11	21.6%
Above 50	1	2%
Total	51	100%

Table 3: Demographic Profile of Age Distribution

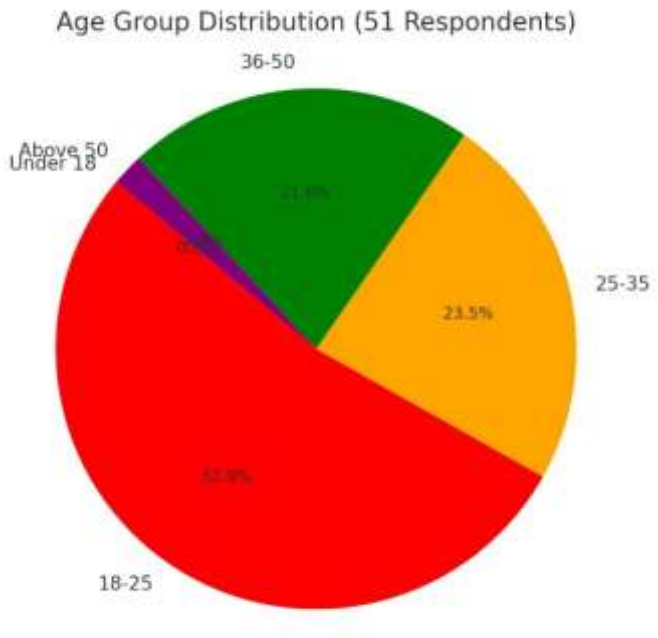

Fig.no.2 Showing Demographic Profile of Respondents

Interpretation:

- Majority of respondents fall in the **18–25** age group, showing a younger demographic involved in the IT sector's HR experiences. This implies digitally aware participants whose opinions reflect the younger workforce's expectations around data privacy and cybersecurity.

- **Belief in Legal Compliance of HR Practices:**

RESPONSE	COUNT	PERCENTAGE
Strongly agree	10	20%
Agree	26	52%
Neutral	8	16%
Disagree	5	10%
Strongly disagree	2	4%
Total	51	100%

Table 4: Belief In Legal Compliance Of HR Practices

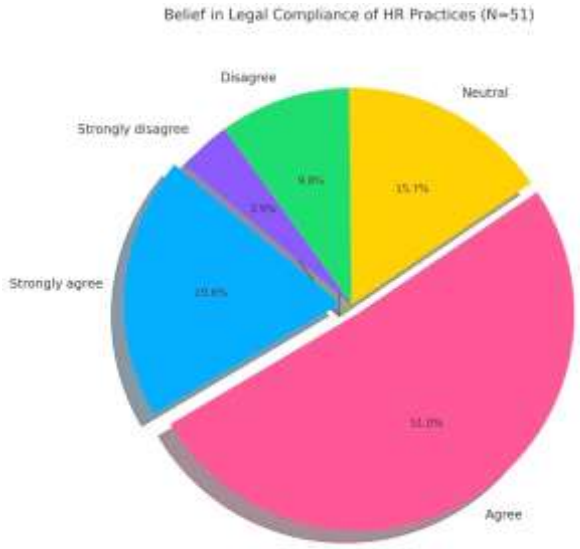

Fig.No.3 Showing The Belief In Legal Compliance of HR Practices

Interpretation:

The data reveals a generally positive sentiment toward HR legal compliance within the IT sector:

- 52% of respondents agreed that their organization's HR practices are legally compliant, suggesting a broad sense of confidence in internal processes.
- 20% strongly agreed, reinforcing this confidence with stronger conviction.
- 16% remained neutral, indicating some uncertainty or lack of information, possibly due to limited exposure to compliance processes.
- A combined 14% disagreed or strongly disagreed, which points to areas needing attention or better communication around compliance measures.

This distribution shows that while most participants trust their HR systems, there's still a need for transparency and education on legal adherence particularly among younger, tech-savvy employees who value ethical governance and digital accountability.

- **Types of Cyber-Attack Experienced by Respondents**

Types of Attack	Count	Percentage
Phishing	8	16%
Ransomware	14	28%
Social Engineering	11	22%
Identity Theft	8	16%
Other	10	20%
Total	50	100%

Table 5: Types of Cyber-Attack Experienced by Respondents

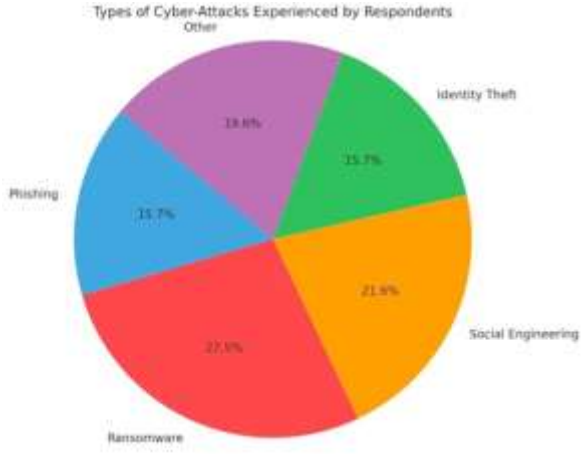

Fig.No.4: Showing the Types of Cyber-Attacks Experienced By Respondents

Interpretation:

- Ransomware is the most commonly experienced cyber-attack, affecting 28% of respondents.
- Social Engineering follows with 22%, indicating a significant concern over manipulation tactics.
- Other attacks make up 20%, showing a variety of additional threats outside the main categories.
- Phishing and Identity Theft are each experienced by 16% of respondents, highlighting the ongoing risk of deceptive communication and personal data compromise.

Ransomware stands out as the leading cyber threat among participants, suggesting a need for stronger backup systems, recovery plans, and employee training. Social engineering's high incidence also indicates a need for awareness programs focused on manipulation and fraud prevention.

CONCLUSION, LIMITATIONS, IMPLICATION AND FUTURE RECMMENDATION

CONCLUSION:

In today's digital-first world, the role of HR in IT companies is no longer just about managing people—it's about managing people's data. This research helped uncover how HR teams are navigating the tightrope of legal compliance, cybersecurity, and ethical responsibility in a landscape shaped by remote work, AI, and increasing data reliance.

There's a clear awareness among HR professionals that cybersecurity and ethics matter. Most know their responsibilities, and many want to do the right thing. But in many cases, that awareness hasn't translated into structured policies, consistent practices, or adequate training. There's a gap between what's expected and what's actually happening.

The conclusion is clear: for HR in the IT sector, data ethics and cybersecurity must become a core part of the HR identity, not just a checkbox during onboarding or compliance season.

LIMITATIONS:

1. Sample Size: The number of survey and interview participants was modest. A larger dataset across more geographic regions or international firms could yield broader insights.

2. Self-Reporting Bias: Since participants reported their own knowledge and practices, there may be social desirability bias people presenting their behavior more positively than it truly is.

3. Focus on HR Professionals Only: This study primarily focused on HR perspectives. Including viewpoints from employees, IT teams, or legal officers could offer a more 360-degree view.

4. Dynamic Legal Landscape: Data laws and cybersecurity threats are constantly evolving. This study is based on current policies (e.g., GDPR, HIPAA, India's DPDP Act) and may need updating as new regulations emerge.

IMPLICATIONS:

The study shows that while HR teams in IT companies are becoming more aware of the importance of data ethics and cybersecurity, there's still a big gap when it comes to putting that awareness into real action. Many HR professionals don't have enough training to deal with cyber threats or to handle sensitive employee data safely, especially when using new technologies like AI. This means companies need to focus more on training their staff and creating clear rules about how employee data should be handled. Employees, especially younger ones, expect their personal information to be kept private and used fairly, so it's important for companies to be open and honest about how they manage data. The study also points out that HR and IT teams need to work together more closely to keep systems secure. For colleges and universities, there's a need to teach students about digital safety and ethical data use so they're better prepared for future jobs. Policymakers can also use these insights to build stronger rules that help protect employee information while still allowing companies to use technology in smart and fair ways.

FUTURE RECOMMENDATIONS:

- Provide regular cybersecurity training for HR professionals.
- Develop and communicate clear data privacy policies.
- Promote employee awareness on data ethics and rights.
- Encourage collaboration between HR and IT departments.
- Conduct regular audits and cybersecurity risk assessments.
- Evaluate AI tools in HR for fairness and transparency.
- Involve employees in shaping data governance policies.

REFERENCES:

Ramesh, P., Bhavikatti, V., Omnamasivaya, B., Chaitanya, G., Tejaswini, Hiremath, S., Gondesi, H. S., & Kameswari, J. (2024). Organisational adaptability: A study of the mediating role of leadership in the influence of strategies, complexity, and technology. International Journal of Innovation Management, 28(1). Read more at: https://doi.org/10.1142/S136391962450002X https://doi.org/10.1016/j.orgdyn.2024.101032

(Ethical considerations of generative AI-enabled human resource management – Organizational Dynamics, 2024)

https://doi.org/10.1016/j.hrmr.2022.100909

(Artificial intelligence and people management: A critical assessment through the ethical lens – Human Resource Management Review, 2023)

https://www.shrm.org/in/topics-tools/news/technology/ethical-implications-of-ai-in-hr--a-comprehensive-analysis (SHRM: Ethical Implications of AI in HR – 2023)

https://www.researchgate.net/publication/381947229_

Ethical_Considerations_in_Artificial_Intelligence_Implementation_for_Human_Resources_Management

Abbas, Z. (2024). Cybersecurity principles in human resources management: Compliance with legal frameworks and ethical considerations. ResearchGate.

https://www.researchgate.net/publication/3820000192.

Junaid, N. (2024). Legal compliance and ethical challenges in cybersecurity for human resources management. ResearchGate. https://www.researchgate.net/publication/382148813

Isabel Ebert et al. (2021) – Big Data in the Workplace: Privacy Due Diligence as a Human Rights-Based Approach to Employee Privacy Protection

https://doi.org/10.1177/20539517211013051

Gatis Polis (2023) – Using the Principles of Cybersecurity Ethics to Mitigate Cybersecurity Risks (Telecom sector, Baltic countries)

https://www.researchgate.net/publication/375075500_USING_THE_PRINCIPLES_OF_CYBERSECURITY_ETHICS_TO_MITIGATE_CYBERSECURITY_RISKS

BM Zahid-ul Haque (2025) – Cybersecurity and Human Resource Management (New Age Bangladesh)

https://www.newagebd.net/post/opinion/270168/cybersecurity-and-human-resource-management

Hassine Riani (2024) – Cybersecurity Ethics (LinkedIn article: fairness, privacy, transparency)

https://www.linkedin.com/pulse/cybersecurity-ethics-hassine-riani-cugnf

Tripwire (2023) – The Importance of Ethics in Cybersecurity

https://www.tripwire.com/state-of-security/importance-ethics-cybersecurity

Fatima Asif et al. (2024) – Ethical Hacking and Its Role in Cybersecurity (ArXiv)

https://arxiv.org/abs/2408.16033

Betsy Uchendu et al. (2021) – Developing a Cyber Security Culture: Current Practices and Future Needs (ArXiv)

https://arxiv.org/abs/2106.14701

Joanne L. Hall & Asha Rao (2024) – Gender of Recruiter Makes a Difference: A Study into Cybersecurity Graduate Recruitment (ArXiv)

https://arxiv.org/abs/2408.05895

Giovanni Apruzzese et al. (2022) – The Role of Machine Learning in Cybersecurity (ArXiv)

https://arxiv.org/abs/2206.09707