International Journal of Economics, Environmental Development and Society, 2025, 6(4), 669-686.

REPOSITIONING HUMAN RESOURCE MANAGEMENT IN EDUCATION FOR THE AGE OF ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

Chinomso Edna OMEZURIKE
Department of Educational Management
Faculty of Education
Ignatius Ajuru University of Education, Nigeria
talk2chinomso@yahoo.com
https://orcid.org/0009-0006-1293-7441

ABSTRACT

The accelerating adoption of Artificial Intelligence (AI) and the rising significance of cybersecurity are profoundly reshaping Human Resource Management (HRM) in the education sector. Traditional HRM functions such as recruitment, training, performance evaluation, and staff welfare are increasingly being mediated by AI-driven technologies that enhance efficiency, predictive analytics, and workforce planning. However, these developments pose significant challenges, including ethical concerns, algorithmic bias, workforce displacement, data breaches, and cyber threats that compromise institutional integrity and employee trust. To address these challenges, HRM in education must be strategically repositioned through comprehensive reskilling and upskilling initiatives, cybersecurity awareness programs, digital literacy integration, and the development of ethical frameworks that promote trust and equity. Policy imperatives should further emphasize regulatory compliance, resilience against cyber risks, and equitable access to AI-enhanced opportunities to ensure inclusivity and sustainability. This paper argues that repositioning HRM in education for the era of AI and cybersecurity is not only a technological adjustment but also a strategic necessity for building resilient, innovative, and future-ready educational institutions.

Keywords: Human Resource Management, Artificial Intelligence, Cybersecurity, Education, Digital Transformation, Workforce Development, Policy Imperatives.

Reference to this paper should be made as follows:

Omezurike, C. E. (2025). Repositioning human resource management in education for the age of artificial intelligence and cybersecurity. *International Journal of Economics, Environmental Development and Society*, *6*(4), 669-686.

 [ISSN: 2992-5614]. DOI: 10.5281/zenodo.18023525.

INTRODUCTION

The rapid infusion of Artificial Intelligence (AI) into educational institutions, coupled with escalating cybersecurity threats, is fundamentally redefining the scope and responsibilities of Human Resource Management (HRM) in the education sector. AI-driven tools have already

begun transforming traditional HR functions, streamlining recruitment, personalizing training, and offering predictive analytics for workforce planning while simultaneously introducing risks of data breaches, algorithmic bias, and workforce anxieties over job displacement (Chauhan & Tyagi, 2025).

As educational institutions increasingly adopt sophisticated HR systems powered by AI, HR professionals must undergo a dramatic shift toward digital fluency, ethical oversight, and cybersecurity readiness. A recent open-access study on public institutions in Tanzania highlights that while AI enhances efficiency, decision-making, and cost-effectiveness, significant barriers persist including lack of expertise, privacy concerns, implementation complexity, and resistance to change (Chauhan & Tyagi, 2025). In a complementary vein, interdisciplinary reviews of AI in HRM emphasize that responsible integration requires AI systems to be explainable, ethically governed, and subject to continuous human oversight (Puranam, 2023; Ahmer & Huang, 2023).

Meanwhile, cybersecurity concerns are mounting. Tech executives overwhelmingly cite cyber threats and data breaches as top business risks prioritizing cybersecurity competencies and AI literacy when hiring staff (Survey of C-Suite execs, June 2025). This underscores the urgent need for HRM strategies that not only harness the transformative power of AI but also protect institutional integrity through cybersecurity awareness and resilient governance (Per Scholas survey, 2025). This paper contends that repositioning HRM in education for the dual imperatives of AI integration and cybersecurity is both a strategic necessity and an ethical obligation. It argues that HR leaders must embrace digital transformation while ensuring ethical AI usage, data protection, workforce upskilling, and policy alignment. By doing so, educational institutions can build HRM systems that are not only efficient but also trustworthy, inclusive, and resilient.

THEORETICAL FRAMEWORK

Human Capital Theory Evolution

Mayilyan and Yedigaryan (2022) discussed the evolution of human capital theory, tracing its development from the conceptual foundations of the new classical theory to its enrichment by institutional, behavioral, evolutionary, and synergetic theories. The theory of human capital, which considers health, knowledge, skills, and motivation as investments that enhance productivity and income, has evolved in response to the changing role of humans in the post-industrial economy. Unlike pre-industrial and industrial economies, where land and capital were the primary production factors, human capital emerges as the most crucial factor in the post-industrial economy. This shift reflects the growing importance of human intellectual and creative potential as sources of development.

Ganush and Tsetsiarynets (2022) explored the evolution of human capital management theories and practices in the educational sector, highlighting the sector's unique challenges and the need for theoretical, methodological, and practical recommendations. The study identifies the main stages of transformation in conceptual aspects of human capital management, correlating with the stages of social, economic, and technical development of the educational sector. This research underscores the importance of a unified concept that reveals the transformation of theoretical and methodological ideas about human capital management within the scientific paradigm corresponding to each historical stage of society's development.

Zhdanov (2023) examined the ontogenesis of human capital within enterprises, applying the four-component system economic theory, the evolutionary theory of the firm, and the theory of human capital. This study identifies key stages in the development cycle of an enterprise's

human capital, demonstrating that the evolution of human capital occurs synchronously with changes in management tasks at each stage of the organization's life cycle. The research highlights the importance of aligning corporate and individual human capital with the demands of each life cycle stage, providing insights into managing human capital evolution effectively.

Kapkaev and Rudenko (2021) discussed the resource-efficient use of human capital in the context of technological changes and sustainable development. The study emphasizes the significance of human capital as a priority resource in the digital transformation era, contributing significantly to productivity growth. It explores the implications of digital transformation for the organization's culture, employee satisfaction, and motivation, highlighting the increasing need to leverage human creativity and potential in the face of routine operation automation.

These bodies of knowledge collectively provide a comprehensive framework for understanding the complex interplay between technological change and human capital evolution, highlighting the need for strategic and adaptive approaches to human capital development in the face of ongoing technological advancements.

CONCEPTUAL CLARIFICATION

Repositioning

Repositioning refers to the deliberate process of restructuring, redefining, or reorienting existing strategies, functions, or practices to adapt to emerging realities, new trends, or evolving needs in order to remain effective and relevant. It involves shifting perspectives, priorities, and actions to align with contemporary demands, technological transformations, and stakeholder expectations (Kotler et al., 2022).

In organizational and educational contexts, repositioning implies rethinking traditional models and practices to enhance competitiveness, relevance, and sustainability in a rapidly changing environment (Al-Hadhrami, 2023). Rather than a total replacement, repositioning often builds on existing strengths while integrating innovation, technology, and policy reforms to achieve desired goals. Applied to Human Resource Management (HRM) in education, repositioning means transforming HR roles from administrative support functions into strategic enablers of digital innovation, workforce resilience, and institutional security, especially in the age of Artificial Intelligence (AI) and cybersecurity challenges (Chauhan & Tyagi, 2025). Also, repositioning is the strategic process of redefining and adapting existing structures, practices, or policies to meet evolving demands and future challenges, while maintaining institutional relevance and sustainability (Kotler et al., 2022).

Human Resource Management (HRM)

Human Resource Management (HRM) refers to the systematic process of recruiting, developing, managing, and retaining employees to achieve organizational goals and ensure sustainable growth. It involves aligning the workforce with institutional objectives by focusing on talent acquisition, performance management, training and development, employee relations, compensation, and workplace well-being (Dessler, 2020).

In the education sector, HRM plays a critical role in ensuring that schools, colleges, and universities have qualified, motivated, and future-ready educators and staff who can respond to the dynamic challenges of globalization, digital transformation, and emerging technologies such as Artificial Intelligence (AI) and cybersecurity systems (Okolie et al., 2023). Modern HRM

goes beyond administrative functions it has become a strategic partner in organizational development, integrating technology-driven tools, data analytics, and ethical practices to support innovation, inclusivity, and long-term competitiveness (Nankervis et al., 2023).

Functions of HRM

- Recruitment and Selection – Attracting and hiring competent staff.
- Training and Development – Building capacity through continuous learning and digital skills.
- Performance Management – Monitoring and improving staff effectiveness.
- Compensation and Rewards – Ensuring fair pay and motivation systems.
- Employee Relations and Well-being – Promoting positive work culture and support.
- Strategic Workforce Planning – Preparing institutions for future challenges, especially in the age of AI and cybersecurity.

Artificial Intelligence

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines and systems that are capable of performing tasks such as reasoning, learning, problem-solving, decision-making, and natural language processing (Russell & Norvig, 2021). In education, AI is increasingly applied in personalized learning, automated grading, administrative efficiency, and predictive analytics to support both teaching and institutional management (Zawacki-Richter et al., 2019; Dwivedi et al., 2023). Also, AI is the development of computer systems capable of performing cognitive functions typically associated with human intelligence such as learning, reasoning, and adaptation (Dwivedi et al., 2023).

AI Developments: Key Advancements in AI Technologies and their Applications in the Workplace

The landscape of artificial intelligence (AI) has undergone significant advancements, profoundly transforming the information and communication technology (ICT) sector. Technologies like machine learning, deep learning, and natural language processing have taken center stage, enabling improvements in communication, digital commerce, content creation, and software development (Goodfellow et al., 2016; Lecun, Bengio, & Hinton, 2015). AI's impact extends beyond mere technical enhancements—it fosters new business models, creating unprecedented opportunities through heightened efficiencies and more intuitive user interfaces. This shift is poised to revolutionize a broad range of industries, from healthcare and bioinformatics to financial services, dramatically altering sales, marketing, supply chain management, and service delivery mechanisms (Jordan & Mitchell, 2015; Russell & Norvig, 2016).

The rapid integration of AI, coupled with advancements such as the Internet of Things (IoT) and blockchain technology, is accelerating industrial and technological transformations worldwide (Atzori, Iera, & Morabito, 2010). These changes are reshaping organizational cultures, driving innovation, and enhancing workplace efficiency. AI's capacity to automate tasks traditionally performed by humans highlights its critical role in creating intelligent systems capable of managing complex processes, thus optimizing operations and improving returns on investment (Marr, 2020). The exploration of AI frontiers, including Machine Learning (ML), Deep Learning (DL), Fuzzy Logic (FL), Natural Language Processing (NLP), and Genetic

Algorithms (GA), showcases the disruptive power of AI across various sectors (Shalev-Shwartz & Ben-David, 2014).

AI's role in marketing is similarly transformative, offering innovations that refine existing strategies and open new avenues for value creation (Davenport, Guha, & Grewal, 2020). Technologies such as programmatic advertising, social media automation, and voice interfaces enable hyper-personalized customer experiences, more efficient ad spending, and deeper analytical insights. However, widespread AI adoption in marketing also raises important concerns around misuse, job displacement, and the ethical challenges posed by advanced automation and data processing (Borgesius, 2018).

The intersection of AI and big data analytics has further transformed industries by enabling businesses to harness vast amounts of information for real-time decision-making (Chen, Chiang, & Storey, 2012). This has been particularly impactful in fields such as healthcare, finance, and retail, where data-driven insights offer significant competitive advantages. For example, predictive analytics powered by AI algorithms can detect financial fraud, recommend personalized treatments in healthcare, or optimize supply chain management (McAfee & Brynjolfsson, 2012). Moreover, AI's integration with big data technologies facilitates the automation of complex tasks that were previously only manageable by human experts, thus improving both the speed and accuracy of critical operations (Kitchin, 2014). However, this increasing reliance on AI-driven data analytics also raises concerns about data privacy and security, particularly in industries that handle sensitive information (Zuboff, 2019).

As AI continues to evolve, one of its most significant advancements lies in its ability to enhance human-machine collaboration. The concept of augmented intelligence, which aims to use AI not as a replacement for human workers but as a tool to complement and enhance human capabilities, has gained traction across industries (Wilson & Daugherty, 2018). In manufacturing, for instance, AI systems work alongside human operators to optimize production processes and reduce errors, while in healthcare; AI assists clinicians in diseases by analyzing medical imaging with a level of precision that was previously unattainable (Davenport & Kalakota, 2019). The collaborative potential of AI in these sectors not only enhances productivity but also helps address skills shortages, particularly in areas requiring specialized expertise (West, 2018). However, as AI systems become more integrated into the workplace, it is essential to ensure that these technologies are designed and deployed ethically to avoid exacerbating existing inequalities in labor markets (Susskind, 2020).

These developments underscore AI's transformative potential across sectors, necessitating ongoing research and ethical frameworks to ensure that its benefits are maximized while mitigating its risks (Brynjolfsson & McAfee, 2017). As AI continues to evolve, it is crucial to address the associated ethical, social, and educational challenges, ensuring that society is prepared to fully harness AI's capabilities in the workplace and beyond. Following the discussion on AI's advancements, additional research highlights the expanding role of human machine collaboration in multiple sectors. In healthcare, for instance, the integration of AI has enhanced medical imaging, enabling machines to outperform humans in detecting diseases like cancer. However, the collaboration between human doctors and AI systems ensures better healthcare outcomes, with doctors using AI for diagnosis while focusing on patient care and treatment planning (McKinsey, 2023). The interaction between humans and machines continues to enhance efficiency without completely replacing human roles in critical fields like healthcare and manufacturing.

Recent studies also emphasize the critical role of AI in decision-making processes. For example, Gebru et al. (2022) explored human-machine trust in decision-making, highlighting

that trust remains an essential component when it comes to integrating AI in workplace environments. Similarly, Rudin et al. (2022) stress the importance of interpretability in AI systems, ensuring that human users understand AI decisions and build a collaborative environment that improves organizational outcomes. Another domain seeing rapid AI adoption is crowdsourcing. This collaborative model involves humans and AI working together to gather and process data, significantly enhancing efficiency in data-heavy industries. Researchers have analyzed how cognitive biases in human decision-making can be managed by AI, improving the quality of crowd-sourced data (Jiao et al., 2020). Incentive mechanisms are being explored to encourage more effective human participation in AI-driven projects (Yun et al., 2021). Thus, these findings underscore that while AI significantly improves operational capacities, the future lies in fostering hybrid teams of humans and machines, complementing human creativity and judgment with AI's computational power.

AI's Implications for Job Roles and Skill Requirements

The survey by Saraswathi et al. (2023) explores the current condition, challenges, and potential applications of AI in human resource management (HRM), highlighting the transformative potential of AI across various HR processes, including learning and development, performance management, employee engagement, and recruitment. The study discusses the use of AI algorithms and machine learning approaches to automate routine HR operations and analyze vast amounts of employee data, providing insightful data to aid decision-making.

However, it also addresses the ethical and legal ramifications of using AI in decision-making processes, such as bias, privacy issues, and transparency, emphasizing the need for responsible design, oversight, and periodic evaluation of AI systems. Morandini et al.'s research investigates the transformation of professional skills by AI, identifying solutions to the challenges that arise from AI implementation in various organizational sectors. The study emphasizes the importance of upskilling or reskilling workers to adapt to new working and organizational models necessitated by AI's potential to automate tasks or reduce cognitive workload. It highlights the critical role played by transversal skills and identifies strategies to support organizations and guide workers toward the upskilling and reskilling challenges, addressing fairness and inclusion posed by age, gender, and cultural diversity.

Employee Engagement and the Impact of Emerging Technologies

Demaci (2022) explored the impact of emerging technologies, including AI, on business models, customer behavior, and workforce implications. The study emphasizes the importance of strategic approaches that consider the wants and fears of customers and employees while fostering growth and innovation. It underscores the significance of investing in retraining and development to equip the workforce with the necessary skills to adapt to new job roles and addresses the importance of collaboration between employees and technology to meet their needs and concerns.

Kumar et al. (2023) delved into the technostress phenomenon at an organizational level from ML and AI deployment, investigating the automation-augmentation paradox and socio-technical systems as coping mechanisms for technostress management among managers. The study identifies role ambiguity, job insecurity, and the technology environment as primary contributors to technostress due to ML and AI technologies deployment. It proposes the integration of ML and AI automation-augmentation interdependence, along with socio-technical

systems, as effective strategies for technostress management, emphasizing the need for technical upskilling of employees and the realization of ML and AI value. These studies collectively highlight the multifaceted implications of AI on human capital, underscoring the need for strategic adaptation, ethical considerations, and continuous learning to harness AI's potential while mitigating its challenges.

Cybersecurity

Cybersecurity is the practice of protecting digital systems, networks, and data from unauthorized access, attacks, or damage through technological, organizational, and human-centered safeguards (Von Solms & Van Niekerk, 2013). In education, cybersecurity ensures the confidentiality, integrity, and availability of sensitive data, such as student records, research databases, and institutional information systems (Sharma et al., 2022). Also, Cybersecurity is the strategic defense of digital systems, infrastructures, and information from cyber threats and vulnerabilities (Sharma et al., 2022). AI drives innovation and efficiency in teaching, learning, and HRM while Cybersecurity ensures safe and ethical use of AI and other digital technologies and without robust cybersecurity, the adoption of AI in education poses risks such as data breaches, identity theft, and academic integrity violations.

Repositioning Human Resource Management in Education

Repositioning Human Resource Management (HRM) in education refers to a strategic reorientation of HR practices, structures, and policies to effectively respond to emerging global trends, particularly the rise of Artificial Intelligence (AI), cybersecurity challenges, digital transformation, and evolving workforce expectations. The traditional HRM model in education focused mainly on recruitment, training, payroll, and staff welfare is no longer sufficient to meet the complexities of 21st-century educational systems. Instead, HRM must be redefined as a driver of institutional innovation, workforce agility, and digital resilience (Chauhan & Tyagi, 2025).

Historically, HRM in education operated as an administrative function, managing personnel records, hiring processes, and compliance. Today, repositioning requires a shift towards strategic HRM, where human resource professionals play a key role in aligning workforce planning with institutional goals such as quality assurance, digital learning integration, and global competitiveness (Puranam, 2023). This means HR leaders must not only manage people but also anticipate how technology and global trends will affect educational staff performance and retention.

Integration of Artificial Intelligence (AI)

AI has redefined HRM by automating recruitment, performance evaluation, and employee training. Educational institutions now deploy AI-powered tools to streamline candidate selection, personalize professional development, and monitor workforce engagement (Ahmer & Huang, 2023). Repositioning HRM means embracing AI responsibly ensuring transparency, fairness, and inclusivity while preventing algorithmic bias and ethical concerns. For instance, AI can predict teacher turnover risks or recommend skill-development programs, but HR professionals must ensure these systems respect equity and data privacy (Brougham & Haar, 2021).

Addressing Cybersecurity Imperatives

With the rise of digital learning and remote education, institutions face growing cybersecurity threats that target sensitive employee and student data. HRM must therefore reposition itself as a custodian of cyber-awareness and resilience by embedding cybersecurity literacy into recruitment, onboarding, and continuous training (Survey of U.S. Tech Executives, 2025). This involves not only technical security but also cultivating an organizational culture of digital responsibility, ensuring that staff understand their roles in preventing data breaches and cyberattacks.

Growing Importance of Artificial Intelligence (AI) in Cybersecurity

Amidst this ever-changing threat landscape, artificial intelligence (AI) has emerged as a powerful tool for enhancing cybersecurity defenses. AI offers the ability to analyze vast amounts of data, detect patterns, and identify anomalies at speeds and scales beyond human capabilities. By leveraging machine learning algorithms and predictive analytics, AI-driven cybersecurity solutions can detect and respond to threats in real-time, helping organizations stay one step ahead of cyber adversaries. As the volume and sophistication of cyber-attacks continue to rise, the role of AI in cybersecurity has become increasingly indispensable, revolutionizing how we approach threat detection, prevention, and incident response.

Workforce Reskilling and Digital Competence

The future workforce in education will require advanced digital skills, adaptability, and interdisciplinary knowledge. Repositioning HRM means prioritizing continuous reskilling and upskilling through professional development programs that prepare educators and administrators for AI-driven learning environments and cybersecurity challenges (Rahman & Sardar, 2024). For example, HR managers must design training models that combine pedagogy, technology, and ethics to ensure that educators remain relevant in fast-changing educational ecosystems.

Policy and Ethical Imperatives

Repositioning HRM demands the creation of policy frameworks that regulate AI use, protect employee rights, and address cybersecurity risks. HRM in education must advocate for ethical standards that balance innovation with human dignity, ensuring that technology complements rather than replaces educators (Responsible AI in HRM, 2024). This also includes equitable access to digital tools to avoid reinforcing existing inequalities in education.

Repositioning Human Resource Management in Education for the Age of Artificial Intelligence and Cybersecurity

Human Resource Management (HRM) in education has traditionally focused on recruitment, training, performance evaluation, motivation, and staff welfare to ensure effective delivery of teaching and learning. However, the emergence of Artificial Intelligence (AI) and the growing importance of cybersecurity are reshaping the way educational institutions manage their

workforce and organizational structures (Dwivedi et al., 2023; Sharma et al., 2022). To remain relevant and effective, HRM in education must be repositioned, reoriented and strategically realigned to harness the opportunities of digital transformation while safeguarding institutions from associated risks.

Importance of Repositioning HRM in Education for the Age of Artificial Intelligence and Cybersecurity

Repositioning HRM in education to integrate AI tools enables institutions to streamline recruitment, workforce planning, and performance evaluation. AI-driven analytics can identify skill gaps, predict staffing needs, and improve data-driven decision-making, which enhances institutional efficiency (World Economic Forum, 2025). Adopting AI, HR managers in education can reduce administrative burdens and focus more on strategic roles that promote teaching and learning outcomes.

Educational institutions process vast amounts of sensitive staff and student data, making cybersecurity central to HRM. Repositioning HR practices to include cybersecurity safeguards ensures protection against data breaches, identity theft, and unauthorized access (Center for Internet Security [CIS], 2024/2025). In Nigeria, the Nigeria Data Protection Act (NDPA) 2023 mandates strict compliance with data security and privacy, making cybersecurity integration into HRM both a legal and ethical necessity (Federal Republic of Nigeria, 2023).

The shift towards AI-driven education requires employees who are digitally literate and capable of working in technology-enriched environments. HRM must reposition to prioritize upskilling and reskilling of teachers and administrators in AI literacy, digital ethics, and cybersecurity awareness (UNESCO, 2025). This prepares the workforce for the Fourth Industrial Revolution, where adaptability and technological fluency are critical.

AI in HRM such as automated recruitment, performance monitoring, and predictive analytics raises concerns about fairness, bias, and accountability. Repositioning HRM ensures that AI tools in education are deployed ethically, with human oversight, transparency, and fairness (National Institute of Standards and Technology [NIST], 2023). This protects institutions from reputational damage and reinforces trust among staff and students.

Cybersecurity threats such as ransomware attacks, phishing, and insider threats are rising in educational institutions worldwide (EDUCAUSE, 2024). HRM must integrate cybersecurity training, incident response preparedness, and risk management into workforce policies. These repositioning builds resilience against disruptions and secures institutional continuity in an increasingly volatile digital environment.

Global education stakeholders, including UNESCO and the WEF, emphasize the importance of leveraging AI responsibly to achieve inclusive, quality education (UNESCO, 2025; WEF, 2025). Repositioning HRM aligns educational institutions with these international standards while supporting national digital transformation strategies. This ensures relevance, competitiveness, and sustainability of education systems in the AI and cybersecurity era.

Historical Perspective of Cybersecurity Threats

The historical perspective of cybersecurity threats provides valuable insights into the evolution of digital security challenges and the necessity for continuous advancements in protective measures. Cybersecurity threats have undergone significant evolution over the past few decades, closely paralleling the rapid advancements in technology. In the nascent stages of computing,

cybersecurity concerns primarily revolved around safeguarding mainframe computers and networks from unauthorized access. During this era, the predominant threats were relatively simple, often manifesting as viruses and worms. These malicious programs were frequently propagated through physical media such as floppy disks, posing a significant risk to early computing systems.

However, with the widespread adoption of the internet, cyber-attacks underwent a paradigm shift, exploiting vulnerabilities in networked systems to propagate and inflict damage. This transition ushered in a new era of cyber threats characterized by the emergence of more sophisticated attack vectors. Malware, including viruses, trojans, and ransomware, became prevalent tools in the arsenal of cybercriminals, capable of infiltrating and compromising systems with devastating consequences. Denial-of-service (DoS) attacks emerged as a means to disrupt the availability of online services by overwhelming target servers with an influx of malicious traffic. Moreover, data breaches became increasingly common, resulting in the unauthorized access and exfiltration of sensitive information from organizations and individuals alike.

Historical incidents such as the Morris Worm of 1988 and the Code Red worm of 2001 serve as poignant reminders of the disruptive potential of cyber threats. The Morris Worm, created by Robert Tappan Morris, infected thousands of computers connected to the early internet, causing widespread system slowdowns and outages. Similarly, the Code Red worm exploited vulnerabilities in Microsoft's Internet Information Services (IIS) web server software, infecting hundreds of thousands of servers worldwide and defacing websites with a message proclaiming “Welcome to http://www.worm.com! Hacked By Chinese!”.

These high-profile incidents underscored the need for robust cybersecurity measures to mitigate the risks posed by increasingly sophisticated cyber-attacks. The historical perspective of cybersecurity threats highlights the evolving nature of digital security challenges and the imperative for organizations and individuals to remain vigilant in defending against malicious actors. As technology continues to advance, cybersecurity strategies must adapt accordingly to address emerging threats and safeguard the integrity, confidentiality, and availability of digital assets.

Current Cybersecurity Risks and Challenges

In today’s interconnected digital world, organizations face a myriad of cybersecurity risks and challenges. Cyber-attacks have become more sophisticated and diverse, targeting not only large corporations but also small businesses and individuals. Ransomware attacks, where cybercriminals encrypt valuable data and demand payment for its release, have proliferated in recent years, causing financial losses and operational disruptions. Phishing attacks, which use deceptive emails or websites to trick users into divulging sensitive information, remain a prevalent threat. Additionally, insider threats, perpetrated by malicious employees or unwitting insiders, pose significant challenges to organizations' cybersecurity posture. Moreover, the increasing adoption of Internet of Things (IoT) devices and cloud computing introduces new attack vectors and amplifies the complexity of cybersecurity management.

CHALLENGES OF REPOSITIONING HUMAN RESOURCE MANAGEMENT IN EDUCATION FOR THE AGE OF ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

Repositioning Human Resource Management (HRM) in education for the realities of Artificial Intelligence (AI) and cybersecurity is not without challenges. In the fast-paced world of cybersecurity, where threats evolve at an alarming rate, the integration of artificial intelligence (AI) brings promises of enhanced defenses and proactive strategies. However, amid this technological marvel, lie a multitude of challenges and limitations that demand meticulous attention. These challenges not only test the technical capabilities of AI systems but also probe the ethical, human, and regulatory dimensions of cybersecurity, while AI promises efficiency, personalization, and predictive analytics, and cybersecurity ensures institutional resilience, the transition raises structural, ethical, financial, and policy-related challenges that HR managers in education must address. The major areas of challenge include:

Technological Skills Gap and Digital Illiteracy/Technical Challenges and Limitations of AI-Powered Defenses

One of the greatest challenges is the lack of digital skills among educators, administrators, and HR personnel. Many staff in educational institutions lack the technical competencies required to adopt AI-driven HR systems or understand cybersecurity protocols (Bond et al., 2021). For example, teachers may be proficient in pedagogy but struggle with AI-based performance monitoring platforms, while HR officers may find it difficult to interpret predictive analytics tools. Without adequate reskilling, the repositioning of HRM risks leaving employees behind. Despite the tremendous potential of AI in cybersecurity, technical challenges and limitations persist. One significant challenge is the adversarial manipulation of AI systems.

Cyber attackers can exploit vulnerabilities in AI algorithms through techniques such as adversarial examples, fooling AI-powered defenses into making incorrect decisions. Moreover, the dynamic nature of cyber threats requires AI systems to adapt and learn in real-time. Achieving this level of agility while maintaining accuracy and reliability poses a considerable technical hurdle. Additionally, the reliance on AI introduces new points of failure, as system failures or vulnerabilities in AI algorithms can be exploited by adversaries.

Resistance to technology adoption, reduced efficiency, and a widened gap between digitally skilled and unskilled staff. Example: In Nigerian universities, studies show that many HR officers still rely heavily on paper-based recruitment and payroll management systems, making the adoption of AI-driven systems more difficult (Adebayo & Oni, 2022).

Ethical and Legal Concerns in AI-driven HRM

AI in HR processes such as recruitment, promotion, or appraisal often raises ethical and fairness concerns. Algorithms may unintentionally reproduce or amplify bias if they are trained on skewed data (Jarrahi et al., 2022). For example, an AI recruitment tool trained on historical hiring data may reinforce gender or ethnic biases. As AI algorithms become more sophisticated, ethical considerations loom large over the cybersecurity landscape. The deployment of AI in cybersecurity raises profound questions regarding privacy, autonomy, and accountability. AI-driven systems often rely on vast amounts of data, leading to concerns about data privacy and potential misuse. Furthermore, the opaque nature of AI algorithms can obscure decision-making

processes, raising questions about transparency and accountability. Ethical dilemmas, such as the trade-off between security and individual freedoms, underscore the need for robust ethical frameworks to guide the development and deployment of AI in cybersecurity.

Many developing nations, including Nigeria, lack comprehensive AI governance frameworks in education, leaving HR practices vulnerable to unethical use of technology (Dwivedi et al., 2023).

Cybersecurity Threats to HR Data/Human Factors in AI-Based Cybersecurity Systems

HRM functions in education rely heavily on sensitive employee data such as payroll, health records, and performance histories. With increased digitization, such data becomes a prime target for cyberattacks, phishing, identity theft, and ransomware (Sharma et al., 2022).

In the realm of AI-based cybersecurity, human factors play a pivotal role in the effectiveness of defense mechanisms. Human operators are tasked with interpreting and acting upon the outputs of AI systems, making decisions that can have far-reaching consequences. However, human-machine interaction introduces complexities and uncertainties. Misinterpretation of AI-generated alerts or overreliance on AI systems can lead to false positives or negatives, undermining the efficacy of cybersecurity defenses. Moreover, the skills gap in understanding AI technologies among cybersecurity professionals poses a challenge in harnessing the full potential of AI-powered systems.

Data breaches can damage institutional reputation, erode trust, and expose staff to identity fraud. Several universities globally have reported cyberattacks that compromised staff and student databases, highlighting vulnerabilities in higher education cybersecurity infrastructures

Problems of Repositioning Human Resource Management in Education for the Age of AI and Cybersecurity

The integration of Artificial Intelligence (AI) and cybersecurity into Human Resource Management (HRM) in education is transformative but also problematic. While it offers efficiency, personalization, and stronger digital defenses, several practical and conceptual problems hinder repositioning HRM for the digital era. These problems can be categorized as follows:

- Many education stakeholders administrators, educators, and HR managers resist adopting AI-driven systems due to fear of job loss, lack of digital literacy, or distrust in automation. For example, AI-powered recruitment and performance management tools raise anxieties about replacing human judgment with algorithms (Okonkwo & Ade-Ibijola, 2021). Also, teachers and non-academic staff often worry that automation will devalue their roles, making change management a persistent challenge (Dwivedi et al., 2023).
- Repositioning HRM requires massive investment in digital infrastructure (cloud systems, AI platforms, cybersecurity defenses). Developing countries, particularly in Africa, face financial limitations in upgrading ICT infrastructure, cybersecurity firewalls, and AI-driven HR systems (Eze et al., 2022). Without adequate funding, digital divides persist between advanced universities and under-resourced institutions.
- As HRM becomes more digitized, educational institutions face growing exposure to cyber-attacks and data breaches. Sensitive staff and student data such as payroll, health

records, and performance metrics can be exploited if not adequately protected (Sharma et al., 2022). Weak cybersecurity policies make institutions easy targets for ransomware and phishing attacks, undermining trust in AI-enabled HRM.

- Repositioning HRM in the digital era requires professionals who are competent in data analytics, AI ethics, and cybersecurity compliance. Most HR managers in education were trained in traditional personnel management, not in algorithmic decision-making or cybersecurity frameworks (Al-Khrabsheh & Aljarah, 2023). Also, upskilling and reskilling are often slow due to limited training opportunities and lack of structured policy guidance.
- AI and cybersecurity introduce new ethical and regulatory problems. AI-driven recruitment tools may reinforce biases if algorithms are trained on discriminatory datasets (Raghavan et al., 2020). Also, Cybersecurity monitoring can raise privacy concerns, as staff may feel they are under constant surveillance and regulatory frameworks in many countries also lag behind in technological changes, leaving HRM without clear compliance structures (Rahman et al., 2023).
- Many ministries of education and universities lack coherent policies linking HRM reforms to digital transformation. Without national cybersecurity strategies and AI adoption roadmaps, HRM units in education operate in silos and make fragmented decisions (Onyema et al., 2020). This misalignment causes duplication of efforts, waste of resources, and inconsistent implementation of digital HRM strategies.
- AI-driven HRM risks excluding staff with low digital literacy or those working in underfunded institutions. For instance, performance evaluation via digital platforms may disadvantage older staff or those in rural areas with limited internet access (Salmon & Ang, 2022). Repositioning HRM without addressing equity concerns can reinforce inequalities within education systems.

Regulatory and Compliance Issues

The deployment of AI in cybersecurity is not immune to regulatory and compliance challenges. The regulatory landscape surrounding AI technologies is still evolving, with few established frameworks specifically tailored to cybersecurity applications. Compliance requirements, such as data protection regulations and industry standards, add layers of complexity to the implementation of AI-powered defenses. Moreover, cross-border data flows and international collaboration in cybersecurity efforts raise questions about jurisdiction and sovereignty. Addressing these regulatory and compliance issues is essential to ensure that AI-based cybersecurity systems adhere to legal and ethical standards while effectively protecting digital assets. AI holds great promise in bolstering cybersecurity defenses, it is imperative to confront the multifaceted challenges and limitations inherent in its integration. Ethical considerations, technical challenges, human factors, and regulatory issues must be carefully navigated to harness the full potential of AI in safeguarding our digital infrastructure. Only through a comprehensive understanding and proactive mitigation of these challenges can we ensure the responsible and effective use of AI in cybersecurity.

STRATEGIES FOR INTEGRATING AI INTO EXISTING CYBERSECURITY

Integrating AI into existing cybersecurity frameworks requires a thoughtful and strategic approach to ensure seamless integration and maximum effectiveness. One strategy is to start

small by implementing AI powered solutions for specific use cases, such as threat detection or incident response, before scaling up to more comprehensive deployments. Collaboration and partnerships between AI developers, cybersecurity vendors, and organizations are also essential for sharing expertise and resources to develop tailored AI solutions that align with the unique cybersecurity needs of different industries and sectors.

Furthermore, organizations should invest in workforce training and development programs to equip cybersecurity professionals with the skills and knowledge needed to effectively leverage AI technologies. This includes training on AI tools and techniques, as well as promoting a culture of continuous learning and adaptation in the face of evolving cyber threats.

The integration of AI into education offers vast potential for automating administrative processes, personalizing learning, and improving workforce efficiency. For instance, AI-enabled recruitment platforms now assist HR managers in identifying and hiring the best candidates using data analytics, reducing bias, and enhancing fairness in the hiring process (Jarrahi et al., 2022). Similarly, AI tools enable predictive analytics to anticipate teacher attrition, improve staff workload distribution, and enhance professional development (Bond et al., 2021). At the same time, the digitization of educational HR processes creates vulnerabilities to cyber threats. Employee data, payroll systems, and institutional records are increasingly stored in digital platforms, making them prime targets for data breaches and ransomware attacks (Sharma et al., 2022). Repositioning HRM thus involves embedding cybersecurity awareness, policies, and practices into every aspect of workforce management.

HR managers in education must ensure that staff acquire the digital competencies required to thrive in AI-driven environments. Continuous professional development should emphasize AI literacy, data ethics, and cybersecurity practices (Popenici & Kerr, 2022). Repositioned HRM will increasingly rely on AI-driven recruitment tools to streamline selection while ensuring ethical use of algorithms to avoid bias. Training programs should also incorporate cyber hygiene practices to build institutional resilience against threats.

Policies governing AI use and cybersecurity protocols are essential to protect staff and students. HR departments must collaborate with IT specialists and policymakers to establish clear guidelines on data protection, AI ethics, and responsible technology use in education (Soomro et al., 2020). Repositioning HRM does not mean replacing staff with machines but leveraging AI to augment human capabilities. For example, AI can handle routine administrative tasks, allowing educators and HR personnel to focus on strategic and interpersonal roles that require human empathy and judgment (Dwivedi et al., 2023).

POLICY IMPERATIVES FOR EDUCATIONAL HUMAN RESOURCE MANAGEMENT

Educational Human Resource Management (EHRM) involves the systematic planning, development, and administration of personnel policies to ensure effective teaching and learning. In the 21st century marked by globalization, technological disruption, and security concerns policy imperatives in EHRM have become essential for aligning education systems with national development goals and global standards. Thus, policy imperatives must involve the following:

- One major policy imperative is the establishment of transparent, merit-based recruitment and retention systems for teachers and non-academic staff. Fair hiring practices reduce nepotism and promote equity, while retention policies such as professional recognition,

career advancement, and incentives ensure staff motivation (OECD, 2024). Without deliberate policy actions, schools risk shortages of qualified teachers, especially in STEM and digital literacy fields.

- Educational systems must adopt policies mandating CPD to equip teachers with emerging skills such as artificial intelligence (AI) literacy, digital pedagogy, and cybersecurity awareness. UNESCO (2025) emphasizes that teacher capacity-building in these areas is a prerequisite for effective and ethical integration of technology in education. National HRM policies should therefore allocate funding and time for structured training programs.
- Given the rise of digital records and AI applications in HRM, policies must enforce strict compliance with data protection laws. For instance, Nigeria's Data Protection Act (2023) obliges educational institutions to safeguard staff and student records against unauthorized access. Integrating cybersecurity policies into HRM frameworks helps protect institutional integrity and builds trust among stakeholders (Federal Republic of Nigeria, 2023; EDUCAUSE, 2024).
- Modern HRM in education must reflect policies that promote gender equality, inclusivity of persons with disabilities, and cultural diversity. Such policies align with the Sustainable Development Goal 4 (Quality Education), which prioritizes inclusive and equitable education (United Nations, 2024). In practice, this means ensuring equal access to promotions, leadership opportunities, and training for marginalized groups.
- EHRM requires policies that establish performance benchmarks for teachers and administrators. These include appraisal systems linked to student outcomes, classroom innovation, and community engagement. According to the World Bank (2024), policy reforms that tie teacher appraisal to professional growth (rather than punishment) yield higher educational quality. Thus, accountability policies should be developmental and supportive.
- As AI and digital tools reshape education, HRM policies must regulate their adoption in recruitment, performance tracking, and student-teacher engagement. NIST (2023) underscores the importance of policy frameworks that govern ethical AI use to prevent bias and ensure transparency. Such policies safeguard educational integrity while enabling efficiency.
- Policies on staff welfare including occupational health, psychological support, and workload management are critical imperatives. Burnout among teachers is a growing challenge globally, exacerbated by post-pandemic realities (WEF, 2025). HRM must adopt proactive well-being policies to maintain productivity and reduce attrition.
- EHRM policies should prioritize the systematic grooming of educational leaders who can manage complexity, innovation, and change. Leadership pipelines ensure succession planning and institutional stability. Effective leadership policies foster resilience and adaptability in school systems (Bush, 2023).

CONCLUSION

Repositioning Human Resource Management (HRM) in education for the age of Artificial Intelligence and cybersecurity is essential for building resilient, innovative, and future-ready institutions. While challenges such as resistance to change, high costs, skill gaps, and ethical concerns persist, strategic investment in digital skills, robust policy frameworks, and strong cybersecurity practices can turn these barriers into opportunities. Ultimately, success will depend

on how well HRM aligns technology with human-centered values to ensure inclusive, secure, and sustainable educational development in the digital era.

Suggestions

- The suggestion to this problem is; Institutions should implement change management programs, including awareness workshops, peer mentoring, and gradual adoption of AI tools. Demonstrating the benefits of AI (e.g., reduced workload, faster recruitment) can reduce resistance. Also, creating a culture of digital trust through leadership communication and employee engagement is key.
- Governments and institutions should pursue Public–Private Partnerships (PPPs) to fund AI and cybersecurity infrastructure. Also, adoption of cloud-based HRM systems and open-source AI solutions can reduce costs and Institutions in low-resource contexts can adopt phased implementation strategies, starting small and scaling up.
- Educational HRM systems must adopt multi-layered cybersecurity strategies: encryption, firewalls, employee cyber hygiene training, and regular audits, Institutions should establish data governance frameworks and comply with national/international privacy laws (e.g., GDPR) and Incident response teams should be in place to handle breaches swiftly.
- Institutions should invest in continuous professional development (CPD) to upskill HR managers in AI, data analytics, and cybersecurity, Collaboration with tech companies and training institutes can provide tailored certifications for HR officers and the government should encourage lifelong learning by integrating digital competencies into HR career pathways.
- Develop ethical guidelines for the use of AI in recruitment, performance evaluation, and decision-making, Institutions should create AI ethics committees to monitor fairness, bias, and accountability and Legal frameworks must be updated to align with emerging challenges in AI and cybersecurity.
- Also, the solution is for Ministries of Education and educational institutions should create harmonized national policies on AI and cybersecurity in HRM, Institutions must align HRM strategies with digital transformation goals to avoid fragmented implementation and Regular policy reviews should ensure responsiveness to new technological developments.
- Solution to the problem is for the governments and institutions should invest in inclusive digital policies, ensuring equal access to devices, internet connectivity, and digital training. **Also,** Special programs should target women, rural educators, and disadvantaged groups to bridge the digital divide and Affordable subsidized digital tools and broadband expansion can enhance equity in access.

REFERENCE

Ahmer, Z., & Huang, K. (2023). Responsible artificial intelligence in human resources management: A review of the empirical literature. *AI and Ethics, 4*(3), 1185-1200.

Al-Khrabsheh, A. A., & Aljarah, A. (2023). Artificial intelligence in human resource management: Opportunities and challenges. *Journal of Human Resource and Sustainability Development, 11*(1), 15-29.

Bond, M., Buntins, K., Bedenlier, S., Zawacki-Richter, O., & Kerres, M. (2021). Mapping research in student engagement and educational technology in higher education: A systematic evidence map. *International Journal of Educational Technology in Higher Education, 18*(1), 1-30.

Brougham, D., & Haar, J. (2021). Smart technology, artificial intelligence, robotics, and algorithms (STARA): Employees' perceptions of our future workplace. *Journal of Management & Organization, 27*(1), 39-54.

Bush, T. (2023). *Theories of educational leadership and management* (6th ed.). Sage.

Chauhan, K., & Tyagi, M. (2025). The impact of artificial intelligence on human resource management. *International Journal of Research and Innovation in Applied Science, 3*(6), 517-522.

Dessler, G. (2020). *Human resource management* (16th ed.). Pearson.

Dwivedi, Y. K., Hughes, L., Kar, A. K., Baabdullah, A. M., Grover, P., & Abbas, R. (2023). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 71,* 102642.

EDUCAUSE. (2024). *2024 EDUCAUSE Horizon Report: Cybersecurity & Privacy Edition.* EDUCAUSE.

Eze, S. C., Chinedu-Eze, V. C., & Bello, A. O. (2022). Enhancing ICT adoption in higher education: A developing country perspective. *Education and Information Technologies, 27*(2), 2241-2267.

Jarrahi, M. H., Kenyon, S., Brown, T., & Sutherland, W. (2022). Human-AI symbiosis in organizational decision making: A review and research agenda. *International Journal of Information Management, 66,* 102533.

Nankervis, A., Rowley, C., Salleh, N. M., & Kamoche, K. (2023). *Asia Pacific human resource management and organisational effectiveness: Impacts on practice*. Routledge.

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0).*

Okolie, U. C., Nwajiuba, C. A., & Opara, B. C. (2023). Human resource management in higher education institutions: Challenges and strategies in a digital era. *Cogent Education, 10*(1), 2184217.

Okonkwo, C. W., & Ade-Ibijola, A. (2021). Chatbots applications in education: A systematic review. *Computers and Education: Artificial Intelligence, 2,* 100033.

Onyema, E. M., Eucheria, N. C., Obafemi, F. A., Sen, S., Atonye, F. G., Sharma, A., & Alsayed, A. O. (2020). Impact of Coronavirus pandemic on education. *Journal of Education and Practice, 11*(13), 108-121.

Popenici, S. A. D., & Kerr, S. (2022). Exploring the impact of artificial intelligence on teaching and learning in higher education. *Research and Practice in Technology Enhanced Learning, 17*(1), 1-13.

Puranam, P. (2023). The future of HR–AI collaboration systems. *Journal of Organization Design, 12*(1), 45-57.

Raghavan, M., Barocas, S., Kleinberg, J., & Levy, K. (2020). Mitigating bias in algorithmic hiring: Evaluating claims and practices. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT'20),* 469-481.

Rahman, M. M., Ismail, N. W., & Ridzuan, A. R. (2023). Digital transformation and HRM: Policy challenges in developing economies. *Journal of Human Resource Management, 11*(2), 23-38.

Rahman, M., & Sardar, Z. (2024). Digital reskilling for the future workforce: Implications for education and training. *Education and Information Technologies*, *29*(2), 2115-2132.

Responsible AI in HRM. (2024). *International Journal of Human Resource Studies, 14*(2), 55-70.

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Salmon, G., & Ang, S. (2022). Digital inequality in higher education: Learning from pandemic responses. *British Journal of Educational Technology*, *53*(6), 1550-1566.

Sharma, S., Badshah, A., & Dhillon, G. (2022). Cybersecurity in higher education: Emerging threats and protection strategies. *Education and Information Technologies*, *27*(10), 14257-14274.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2020). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 50*, 38-51.

Survey of U.S. tech executives: Cyberattacks reshape hiring priorities-64% call them greatest business threat; 53% prioritize cybersecurity in hiring; 48% see AI integration as major challenge. (2025, June 24). *Per Scholas / Talker Research*. Retrieved from https://nypost.com/2025/06/24/tech/cyberattacks-reshape-hiring-priorities-for-tech-executives

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education-where are the educators? *International Journal of Educational Technology in Higher Education, 16*(1), 39.