European Research Studies Journal
Volume XXVII, Issue 4B, 2024

pp. 567-577

Digitalization as an Essential Area of Security and Management in Modern Organizations

Submitted 12/10/24, 1st revision 21/10/24, 2nd revision 11/11/24, accepted 25/11/24

Zbigniew Ciekanowski[1], Leszek Elak[2], Aneta Chrząszcz[3], Wiesława Załoga[4], Stanisław Marciniak[5]

Abstract:

Purpose: *The purpose of this article is to examine the impact of digitization on security in human resource management. The article discusses the influence of digitization on human resource management in the context of security, analysing key processes and technologies used in modern HRM. The first part explains the concept of HR digitization and describes the main digital tools, such as ATS systems, performance management tools, and LMS platforms, which are changing the ways in which recruitment, development, and evaluation of employees occur. The next section presents the main threats associated with digital HRM, such as data leaks, identity theft, and the risk of unauthorized access, which are becoming increasingly common in light of growing automation and cloud data storage. The third part discusses security measures that include encryption, access authorization, regular audits, and the necessity of compliance with legal regulations such as GDPR, as well as the importance of cybersecurity training. The final section analyses future challenges in digital HRM, highlighting the need for investment in new technologies.*
Design/methodology/approach: *The article formulates the following research problem: How does digitization affect security in human resource management within an organization? It also establishes the following research hypothesis, which posits that the application of appropriate technologies and protective procedures significantly reduces the risk of security breaches in digital HRM, thereby increasing security levels. The article employs theoretical methods based on literature analysis and documents related to digitization and security in HRM, as well as legal regulations such as GDPR, allowing for the identification of key trends, threats, and recommendations in the studied area.*
Findings: *Given the dynamic development of technology and evolving threats in cyberspace, further research is necessary on the impact of new technologies such as artificial intelligence and predictive analytics on digital HRM security. Additionally, the increasing use of cloud data processing necessitates in-depth analyses regarding appropriate protection methods*

[1]*Faculty of Economics, John Paul II University in Biala Podlaska, Poland, ORCID: 0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl;*
[2]*War Studies University Warsaw, Poland, ORCID 0000-0002-5255-9768, l.elak@ron.mil.pl;*
[3]*Faculty of Economics, John Paul II University in Biala Podlaska, Poland, ORCID: 0000-0001-9749-274X, e-mail: aneta.chrzaszcz@op.pl;*
[4]*Military University of Technology, Warsaw, Poland, ORCID: 0000-0001-7758-0187, e-mail: wieslawa.zaloga@wat.edu.pl;*
[5]*Warsaw Management University, Poland, ORCID ID: 0000-0003-0406-1487, e-mail: s.marciniak2@wp.pl;*

and effective risk management strategies. Further studies should also consider new legal regulations and standards that may affect data security practices in HR so that organizations can effectively adapt their actions and minimize breach risks.
Practical Implications: *Effective data protection in digital HRM requires a comprehensive approach that encompasses both modern technologies and appropriate organizational procedures. Key protective measures include encryption, access authorization, and compliance with legal regulations such as GDPR, which form the foundation of data security in this area. The role of cybersecurity specialists and employee education regarding digital threats is equally crucial for the entire organization.*
Originality/Value: *In light of challenges, digital HR is becoming an area that requires not only modern technological solutions but also continuous analysis and risk management to ensure information security and build employee trust in the company. A proper approach to security in digital HRM is essential today and plays a key role in maintaining an organization's reputation as well as protecting its human resources*

Keywords: *Security, digitization, organization, human resource management*.

JEL codes: *O32, M12, M15*.

Paper type: *Research article.*

1. Introduction

The digitalization of Human Resource Management (HRM) transforms the way organizations recruit, develop, and manage employees by introducing modern technologies into everyday processes. The introduction of digital tools in HRM, such as Applicant Tracking Systems (ATS), performance management platforms, and online learning solutions (LMS), significantly enhances the efficiency and accuracy of HR activities, accelerating processes and enabling more strategic personnel management. However, this digital transformation also brings new challenges, particularly concerning the security of personal data and sensitive information.

The application of technology in HR means that vast amounts of information—from personal data to salaries and evaluation results—are processed and stored in digital systems. In light of threats such as data breaches, identity theft, and hacking attacks, organizations must ensure the implementation of appropriate security measures to protect employee data and comply with data protection regulations, such as GDPR.

Given these challenges, digital HR becomes an area that requires not only modern technological solutions but also continuous analysis and risk management to ensure information security and build employee trust in the company. A proper approach to security in digital HRM is essential today and plays a crucial role in maintaining the organization's reputation and protecting its human resources.

2. Digitalization in HRM - Definition and Key Processes

Digitalization in the economic sphere, including management, is one of the most dynamic changes of our time, opening new possibilities for creating business models while also presenting various threats related to the social consequences of process automation and broadly understood security (Wziątek-Staśko, 2022, p. 11).

Changes in the external environment of a company are among the determinants of its functioning, over which companies have relatively little influence (Ciekanowski and Nowicka, 2019, p. 28; Velinov *et al.*, 2023; Grima *et al.*, 2023).

Digitalization of Human Resource Management (HRM) refers to the implementation of modern technologies and digital tools that automate and support various processes related to personnel management. By utilizing these tools, HR departments can not only manage employee data more effectively but also significantly increase the efficiency of their activities, make better decisions, and optimize organizational time and resources.

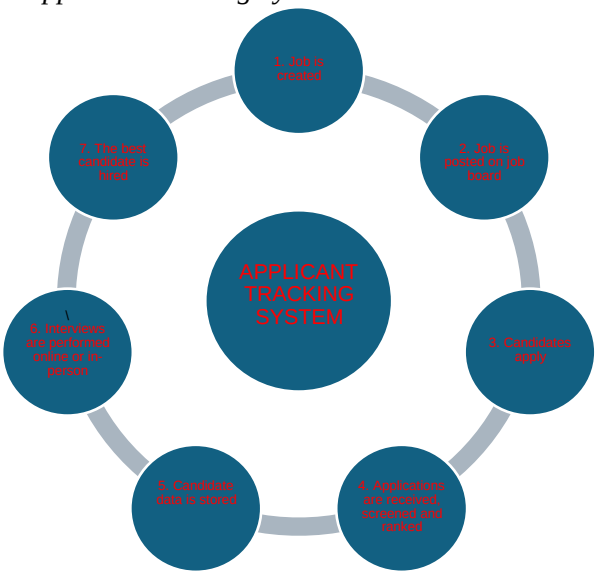
The digital transformation in HR is now a groundbreaking step that changes how employees are managed throughout their employment cycle—from recruitment to professional development to performance evaluation. Below is a diagram illustrating the key elements of HRM.

Figure 1. *Key HRM elements*

Source: *Next Innovation Asia, https://nextinnovationasia.com/.*

Employees are the key capital of modern enterprises (Glišović, Jerotijević, and Jerotijević, 2019; Nafei, 2016; Souleh, 2014). In the context of digitalization, several technologies particularly influence the functioning of HR. One of the fundamental tools used in the digital recruitment process is Applicant Tracking Systems (ATS). These systems provide a comprehensive solution that automates many activities related to talent acquisition. Below is a diagram illustrating how applicant tracking systems work.

Figure 2*. How Do Applicant Tracking Systems Work?*



Source: *Applicant Tracking System (ATS), Bullhorn, https://www.bullhorn.com/uk/glossary/applicant-tracking-system/*

Thanks to ATS, the HR department can effectively manage candidate applications, which are automatically sorted and stored in the system (Tiwari, Vaghela, Nagar, and Desai, 2019, p. 320). This significantly speeds up the selection process as it allows HR specialists to quickly identify candidates with the appropriate qualifications and experience. ATS also enables precise analysis of application data, allowing recruiters to better match candidates to job requirements. This system also streamlines communication with candidates, increasing the transparency of the entire process and reducing wait times for responses, which improves the experience for applicants and positively affects the organization's image.

Another important tool is performance management systems. Such solutions enable the HR department to monitor the effectiveness of teams and individual employees, which is particularly important for organizations that care about developing competencies among their employees. With performance management tools, employers can create systematic work evaluations, allowing for ongoing monitoring of results.

These systems also support the creation of individual development plans, enabling better alignment of development activities such as training, mentoring, or coaching with the needs of specific employees. Moreover, these tools allow for the analysis of performance indicators, helping managers and HR specialists make informed decisions regarding promotions, raises, or corrective actions.

One of the key solutions used in employee development is Learning Management Systems (LMS). LMS allows organizations to effectively manage the education and professional development process of employees by providing access to a variety of online training and courses (Bradley, 2021, p. 68).

With these platforms, employees can learn anytime and anywhere, eliminating the need for time-consuming and costly in-person training sessions. LMS also provides the ability to monitor employees' learning progress, allowing the HR department to continuously control competency development within the company. Below is a diagram illustrating the reasons why it is worthwhile to implement a learning management system.

Figure 3. *Reasons to Implement a Learning Management System.*

Source: *Implementing LMS in Educational Institutions, https://www.classe365.com/blog/implementing-learning-management-systems-in-educational-institutions/*

Moreover, these platforms allow for the creation of individual development paths tailored to the needs and career goals of specific individuals, which significantly

enhances the effectiveness of training processes and develops talents in line with the company's requirements.

Over the years, the conditions under which work is performed have changed. The tools used in work have also evolved (Steinerowska-Streb and Wronka-Pośpiech, 2022, p. 65). Therefore, digitalization has a huge impact on key areas of human resource management, such as recruitment, professional development, and performance evaluation. In the area of recruitment, digital technologies enable the streamlining of the selection process and establishing contact with candidates, which increases efficiency and reduces costs associated with searching for employees.

Regarding professional development, LMS platforms allow for the personalization of educational paths and easier access to training materials, which promotes the development of employee competencies. Performance management systems, on the other hand, enable better monitoring of work outcomes and support the creation of more complex development programs tailored to employee needs. Thus, HR digitalization is not only about tools but also about the ability to respond more quickly to the needs of employees and organizations, ultimately contributing to better performance and competitiveness for the company.

3. Threats to Security and Security Measures in the Digital HR Environment

Digitalization in Human Resource Management brings numerous benefits, but at the same time introduces new challenges and threats regarding data security. In the digital HR environment, securing sensitive information, such as employee personal data, salary information, and details about employee performance and health, becomes particularly important. With the growing use of modern technologies, the risk of personal data breaches and identity theft also increases (Ciekanowski, Nowicka, Czternastek, Żurawski, and Mikosik, 2024, p. 456).

Such incidents can occur when HR systems are inadequately secured or when unauthorized individuals have access to data. They often result from hacking attacks, including phishing, malware, or software vulnerabilities that criminals exploit to gain access to confidential information. The loss of such data can lead not only to financial loss but also to violations of employee privacy and a negative impact on the company's reputation (Tyagi *et al.,* 2023).

Another significant threat is unauthorized access to data, which can result from improper management of permissions and access controls. In many cases, employees who should not have access to sensitive information may accidentally or intentionally reach it if access management systems are not properly configured. While automating HR processes increases efficiency, it can also generate new threats when systems operate without adequate oversight.

Improperly configured automation can lead to situations where data is accidentally sent or disclosed to unauthorized recipients.

Particular risks are also associated with processing data in the cloud, which, although it offers enormous opportunities for scalability and access to information, can increase the risk of external attacks and data breaches. In the case of cloud services, it is crucial for service providers to offer appropriate security measures because storing employee personal data outside the company's infrastructure can involve the risk of losing control over that information. Therefore, ensuring the security of cloud data processing requires special measures such as encryption and strict access control.

To counter these threats, it is necessary to implement effective security measures in digital human resource management (Ciekanowski, Żurawski, and Król, 2023, p. 128). One of the most important elements in protecting employee personal data is implementing encryption protocols that secure data both during storage and transmission. With encryption, data becomes unreadable to unauthorized individuals even if they gain access to it.

Another important aspect is access authorization—permission management systems that allow for strict control over who has access to employee data and to what extent. Proper access management should be based on the principle of least privilege, meaning employees have access only to the data necessary for performing their duties.

Regular security audits are another element that allows for detecting potential threats and vulnerabilities. Through audits, companies can respond promptly to emerging threats and implement appropriate corrective measures before an incident occurs. These audits should include assessments of both technology and procedures as well as security policies employed by the company.

Equally important in securing digital HR environments is compliance with personal data protection regulations such as GDPR (General Data Protection Regulation) in the European Union. GDPR requires organizations to follow specific procedures regarding the processing and protection of personal data, including informing employees about their rights and securing data against unauthorized access. Adapting HR systems to comply with GDPR requirements and other legal regulations is crucial for minimizing legal risks and ensuring compliance with applicable laws.

In addition to technology and procedures, training employees in cybersecurity plays a significant role in protecting data in digital HR (Ciekanowski, Żurawski, Pauliuchuk, Ciekanowski, and Marciniak, 2024, p. 375). Employees are often the first line of defense against threats, and a lack of awareness regarding security can lead to situations where they inadvertently contribute to data breaches by clicking on

dangerous links or sharing information with unauthorized individuals. Cybersecurity training helps raise employee awareness and teaches them how to recognize and avoid potential threats such as phishing, social engineering, or other forms of online fraud.

In summary, security measures in digital human resource management must encompass both modern technologies and appropriate policies as well as employee education. By combining these actions, organizations can effectively protect employee data while ensuring compliance with regulations and enhancing security within their HR structures.

4. Challenges and Future Security in HRM Digitalization

Digitalization of HRM is still developing dynamically, introducing new technologies that not only optimize the work of HR departments but also significantly change the approach to managing personal data. As a result, numerous challenges arise in ensuring the security of sensitive information, which becomes a target for attacks and abuses (Do *et al.*, 2022).

One of the main trends in digital HRM is the increasing automation of processes, from recruitment to performance management and employee development, which requires increasingly advanced systems for storing, processing, and protecting large amounts of data. The introduction of such technologies requires special attention to security, as attacks on HR systems can lead to serious privacy violations as well as financial and reputational losses.

In response to growing security threats, investments in data protection technologies are gaining increasing importance. Organizations are beginning to recognize the necessity of implementing modern solutions such as advanced encryption systems, security monitoring tools, and multi-factor authentication technologies. Such investments help secure data against unauthorized access and enhance employee privacy protection. Companies that prioritize data security gain greater trust from their employees and clients, which is becoming increasingly important in today's globalized and data-driven environment.

Cybersecurity specialists are beginning to play a key role in managing HR data security, collaborating with HR departments on implementing data protection policies and procedures. Until recently, IT and HR security issues were treated as separate areas; however, cybersecurity specialists are now an integral part of HR teams, helping to ensure data security from both technological and legal perspectives. Their role is particularly significant in the context of compliance with legal regulations such as GDPR, which imposes an obligation on organizations to protect employee personal data. These specialists assist HR in conducting regular security audits, assessing risks, and providing security training for the entire organization.

Looking to the future of digital HRM, it can be predicted that new technologies will increasingly impact data security issues. Artificial intelligence and machine learning, which are used for automating recruitment processes and performance evaluations, can potentially help predict and prevent security threats.

An example could be the application of algorithms that detect suspicious activities in real time, allowing for immediate responses to potential threats. At the same time, the development of cloud technologies means that more companies will store data in the cloud, which will require even more advanced protective measures, especially since attacks on cloud infrastructure can have wide-ranging and unpredictable consequences.

The increasing competition among businesses means that achieving sustainable competitive advantage largely depends on creating a unique team of employees (Jawor-Joniewicz 2016, p. 39). The report "State of AI and Automation in HR 2024" highlights as many as 12 challenges for the HR department:

- Planning career paths for employees
- Authentic inclusivity
- Supporting employees in the future workplace (including technology use)
- Maintaining high productivity among employees
- Generation Z in the job market
- Sustainable human resource management policies
- Attracting talent within appropriate timeframes and budgets
- Measuring ROI (Return on Investment)
- Monitoring roles within the organization that provide disproportionate value relative to investment
- Real-time communication with employees—quickest and most effective
- Monitoring employee well-being
- Working on employee engagement (State of AI and Automation in HR 2024 inFeedo).

It is also worth mentioning ongoing technological changes leading to automation of work processes, robotization, and the use of artificial intelligence or the increasing importance of technological and digital competencies that are changing working conditions. Challenges may also include generational diversity among employees, building engagement at work, and changing forms of work provision (Myjak, 2023, p. 109). The evolution of digital HRM will also lead to greater personalization and integration of data, which poses further challenges regarding security for companies.

In the future, HR systems will likely become increasingly integrated with other organizational systems, requiring advanced protections at the entire IT infrastructure level. Integration with external systems such as recruitment or training platforms will also necessitate enhanced protection to prevent potential data leaks.

Digital HRM is an area that is continually evolving and requires an appropriate approach to data protection. Investments in security technologies, the growing role of cybersecurity specialists, and appropriate adjustments to upcoming technological trends and challenges are crucial for ensuring data security in HR. In the context of the future of digital HRM, it can be expected that technologies such as artificial intelligence, predictive analytics, and cloud computing will shape how organizations protect their employees' data while striving for greater integration and personalization as well as increased effectiveness in countering cyber threats.

5. Conclusions

Digitalization of human resource management brings numerous organizational benefits, including the streamlining of recruitment processes, performance management, and employee development. However, as it progresses, new challenges arise, particularly concerning personal data protection. Analyses indicate that effectively securing data in digital HRM requires a comprehensive approach that encompasses both modern technologies and appropriate organizational procedures.

Key protective measures include encryption, access authorization, and compliance with legal regulations such as GDPR, which form the foundation of data security in this area. The role of cybersecurity specialists and employee education regarding digital threats is also crucial, as these elements can be critical for the entire organization.

Considering the dynamic development of technology and evolving threats in cyberspace, further research is necessary to understand the impact of new technologies, such as artificial intelligence and predictive analytics, on the security of digital HRM.

Additionally, the increasing use of cloud data processing necessitates in-depth analyses regarding appropriate protection methods and effective risk management strategies. Future studies should also account for new legal regulations and standards that may influence data security practices in HR, enabling organizations to effectively adapt their actions and minimize the risk of breaches.

References:

Bradley, V.M. 2023. Learning Management System (LMS) Use with Online Instruction. International Journal of Technology in Education, Vol. 4, No. 1, 68-92.

Ciekanowski, Z., Nowicka, J. 2019. Generacyjne wyzwania w zakresie funkcjonowania współczesnych organizacji, Nowoczesne Systemy Zarządzania.Tom 14, nr 1, 27-38.

Ciekanowski, Z., Nowicka, J., Czternastek, M., Żurawski, S., Mikosik, P. 2024. How Cybersecurity Shapes Effective Organizational Management. European Research Studies Journal, Volume XXVII, Issue 2, 454-464.

Ciekanowski, Z., Żurawski, S., Król, A. 2023. Budowanie strategicznego podejścia do zarządzania zasobami ludzkimi. In: Współczesne wyzwania w zarządzaniu

przedsiębiorstwem w erze cyfrowej, red. Ciekanowski, Z., Kacprzak, A. Król, A., Warszawa: Wydawnictwo im. Profesora Leszka J. Krzyżanowskiego Menadżerskie Akademii Nauk Stosowanych w Warszawie.

Ciekanowski, M., Żurawski, S., Pauliuchuk, Y., Ciekanowski, Z., Marciniak, S. 2024. Strategies for Effective Cybersecurity Management in Organizations. European Research Studies Journal, Volume XXVII, Issue 1, pp. 365-379.

Do, T.D., Pham, H.A.T., Thalassinos, E.I., Le, H.A. 2022. The impact of digital transformation on performance: Evidence from Vietnamese commercial banks. Journal of risk and financial management, 15(1), 21.

Glišović, M.A., Jerotijević, G, Jerotijević, Z. 2019. Modern approaches to employee motivation. Економика, 65(2), 121-133.

Grima, S., Thalassinos, E., Cristea, M., Kadłubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital transformation, strategic resilience, cyber security and risk management. Emerald Publishing Limited.

Jawor-Joniewicz, A. 2016. Budowanie zaangażowania pracowników z uwzględnieniem zarządzania różnorodnością, Zarządzanie Zasobami Ludzkimi, Issue 3/4, 39-51.

Myjak, T. 2023. Zmiany i wyzwania w realizacji funkcji personalnej przedsiębiorstw, nr. 3-4, ss. 108-122.

Nafei, W.A. 2016. Organizational Silence: A Barrier to Organizational Change. Case Studies Journal, 5(9), ss. 86-105.

Raport State of AI and Automation in HR. 2024.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Souleh, S. 2014. The Impact of Human Capital Management on the Innovativeness of Research Center: The Case of Scientific Research Centers in Algeria. International Journal of Business and Management, 2(4), 80-96.

Steinerowska-Streb, I., Wronka-Pośpiech, M. 2022. Motywowanie pracowników w dobie cyfryzacji. Zarządzanie Zasobami Ludzkimi, nr 3-4, 56-70.

Tiwari, A., Vaghela, S., Nagar, R., Desai, M. 2019. Applicant Tracking and Scoring System. International Research Journal of Engineering and Technology, Volume 06, Issue 04, 320-324.

Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E., Thalassinos. E. (Eds.). 2023. Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy. Emerald Publishing Limited.

Velinov, E., Kadłubek, M., Thalassinos, E., Grima, S., Maditinos, D. 2023. Digital Transformation and Data Governance: Top Management Teams Perspectives. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (Vol. 111, pp. 147-158). Emerald Publishing Limited.

Wziątek-Staśko, A. 2022. Neuroprzywództwo – nowy wymiar zarządzania ludźmi w erze cyfryzacji. Zarządzanie Zasobami Ludzkimi, nr. 3-4, 10-22.