Applied Journal of Economics, Law and Governance https://doi.org/10.57017/ajelg.v1.i2(2).06

Human Resource Competencies in Healthcare Cybersecurity: Risk Management and Legal Compliance Implications

Ionuț RIZA
Faculty of Law, Economics and Administrative Sciences, Craiova
Spiru Haret University, Romania
https://orcid.org/0000-0002-6977-7729

Anca Mădălina BOGDAN
Faculty of Law, Economics and Administrative Sciences, Craiova
Spiru Haret University, Romania
https://orcid.org/0000-0003-2019-5960

Abstract

The aim of the research was to contribute to the expansion of knowledge on human resources competencies, in order to prevent the emergence and propagation of risks at the organizational and cyber levels. The practical analysis used quantitative-comparative analysis within public and private medical units in Romania, presenting in detail the human resources competencies necessary for risk management. The results indicate that mandatory human resources competencies exert a significant influence on cybersecurity readiness through general and specific competencies, such as IT&C skills, security ethics, and economic competencies. Furthermore, the study highlights critical legal implications regarding GDPR compliance and data privacy liability. The originality of the study is supported by the conclusions resulting from the analysis of the capacity of human resources to integrate theoretical knowledge with practical competencies in the process of cyber risk perception and management. From the perspective of future research directions, the need to identify appropriate methods for assessing the competencies acquired by human resources, applied specifically in the context of cyber risks, is emerging.

Keywords: human resource management; cybersecurity risk; healthcare sector; GDPR compliance; competency framework.

JEL Classification: M12; M15; I8; K24.

Introduction

In the context of risk, a concept, recognized strategically as having fundamental management importance, as well as major importance for other fields, such as economics, sociology, psychology, legal sciences or information security. The increasing complexity of the economic and social environment, the accelerated dynamics of technological change and the increasingly pronounced interdependencies between systems lead to an amplification of uncertainty, transforming risk into a central variable of the decision-making process. The concept of risk is, by its nature, difficult to define precisely, having an elusive and multidimensional character, because it refers to a complex set of interdependent factors, which

can generate different effects depending on the context. Risk does not manifest itself uniformly, but takes on various forms, determined by the field of activity, the organizational specificity, the regulatory framework and the behaviour of the actors involved. For this reason, the conceptualization and perception of risk raises numerous theoretical and methodological difficulties, the definitions existing in the specialized literature can be clearer or, on the contrary, more ambiguous, depending on the perspective from which the phenomenon is analysed and the field of applicability considered. In recent decades, there has been an increasing concern for the study of how both society and organizations relate to risk, not only from a technical perspective, but also from a behavioural and cultural one. Recent research has investigated the hypothesis of the existence of a relatively stable individual predisposition, known as risk propensity, highlighting the fact that the assumption or avoidance of risk can be influenced by personality factors, professional experience, level of education, subjective perception of uncertainty and organizational norms.

Thus, behaviour towards risk is not exclusively the result of rational calculations, but also reflects profound psychological and social dimensions. From this perspective, the notion of risk emerges as a key concept for multiple disciplines, which must be rigorously analysed and integrated in order to be adequately understood. Especially in the field of management, risk is no longer privileged exclusively as a threat, but also as a potential source of opportunities, to the extent that it is identified, assessed and managed developed. Risk management, in this sense, a systematic system through which risks become visible, known and understandable, allowing organizations to learn from previous experiences and develop effective prevention and control measures. At the same time, risk management facilitates a fundamental and rational decision-making process, by reducing uncertainty and by integrating relevant information into organizational strategies (Sayvaya & Siagian, 2024). The approach of risk in a structured way, determine organizations to anticipate potential dysfunctions, limit the impact of negative events and strengthen their ability to adapt in an environment characterized by volatility and continuous change. In this context, risk becomes not only an element of analysis, but also an essential tool for ensuring long-term organizational sustainability and performance.

Organizations can monitor AI risks effectively by implementing a combination of proactive and reactive strategies, such as structured forecasting methods like the Delphi method, automated monitoring tools, system logs, user feedback, regular audits, and participation in regulatory sandboxes. These measures help identify, assess, and mitigate risks throughout the AI system's lifecycle, ensuring compliance with legal requirements and safeguarding individual rights (Almada, 2024).

The scientific approach of the research had as its starting point the clarification of the role and importance of human resources in risk management, with the aim of outlining a more coherent and comprehensive picture of the complexity of this process, both at the organizational and cyber levels. In a context marked by accelerated digitalization and the intensification of cyber threats, human resources are becoming a determining factor in the identification, prevention and management of risks, going beyond the traditional role of simple executor of security procedures (Chodyka et al., 2025).

The decision-making problem that underpins the research is formulated around the essential question: what is the role of the fundamental competencies of human resources from the perspective of cyber risk management, analysed at the organizational level? The answer to this question requires an integrated approach, which correlates the dimension of professional competencies with the capacity of organizations to deal with increasingly sophisticated cyber threats.

From a theoretical point of view, the article proposes a perspective oriented towards the way in which human resource competencies are perceived in relation to cyber risk at the organizational level. This approach is distinguished from the dominant directions in the specialized literature, which mainly focus on the definition and description of the concept of risk management, paying less attention to the active role of human resources and their competency dimension in the management of cyber risks.

The essential role of the article consists in highlighting and substantiating the need to develop specific competencies in the field of cyber risk management at the organizational level, this need being outlined as one of the major requirements of the contemporary employee. In this sense, cybersecurity competencies can no longer be considered exclusively the prerogative of IT specialists, but must be integrated into a broader set of fundamental human resource competencies, indispensable for ensuring organizational resilience and long-term sustainability.

1. Literature Review

Most definitions established in the scientific literature approach risk as a combination of the probability of an undesirable event occurring and the severity of its associated consequences. From this perspective, risk is expressed as a direct relationship between the possible frequency of the manifestation of a dangerous situation and the negative impact that it can generate on the individuals, organizations or systems analysed. Thus, determining risk involves assessing the degree of probability that an incident will occur and estimating its potential effects, if it materializes (Drozdowski et al., 2021).

In practice, however, the capacity of human resources to accurately forecast such situations and to make objective calculations regarding risk is limited by cognitive, experiential and contextual factors. Decisions are not always based exclusively on rational analyses or mathematical models, but are influenced by subjective perceptions, the level of knowledge, time pressure and the organizational framework in which individuals act. Consequently, risk estimation is not only a technical exercise, but also a deeply human process, marked by personal interpretations and judgments (Szczepaniuk & Szczepaniuk, 2022). In reality, the ability to appreciate risk in a specific situation is determined by several successive and interdependent stages.

The first stage is the perception of risk, corresponding to the identification phase, in which the individual recognizes the existence of a potential threat. This is followed by the risk assessment, a stage that involves a subjective analysis of the probability and possible impact, based on available information and previous experience. Finally, risk tolerance reflects the personal level of acceptance of uncertainty and potential consequences, influencing the decision to assume, avoid or transfer the risk (Nurse et al. 2025). Therefore, risk cannot be understood exclusively as an objective, quantifiable variable, but must also be analysed from the behavioural perspective of human resources. The integration of perceptual and attitudinal dimensions in the risk management process is essential for the development of effective

prevention and control strategies, especially in contexts characterized by complexity and high uncertainty.

Recent studies in the literature highlight the fact that the perception, assessment and assumption of risk are processes influenced by a combination of individual and situational factors. Thus, the personality, stable psychological traits and emotional disposition of the individual play a significant role in the way in which risk is interpreted and managed. Factors such as previous experience, level of self-confidence, tolerance for uncertainty or cognitive style can amplify or diminish the perception of danger, implicitly influencing the decisions taken in risky contexts. In addition to the individual dimension, research highlights the determining importance of the context in which the risk situation occurs (Zhang et al., 2024).

The specific characteristics of the circumstances, the degree of urgency, the complexity of the available information and the anticipated consequences contribute to the formation of a subjective assessment of risk, which is not always aligned with the objective assessments made through technical or statistical methods. At the same time, a series of studies highlight the fact that the social group, especially at the organizational level, exerts a considerable influence on individual attitudes towards risk. Informal norms, organizational culture, managerial practices, and prevailing behaviours within the team can shape how employees perceive risk and decide to assume or avoid it.

Thus, risk is not only an individual construct, but also a social one, resulting from the interaction between the individual and the organizational environment (Dawson, 2018). In this context, risk management must take into account not only the technical competencies of human resources, but also the psychosocial influences that can favour or inhibit responsible behaviour towards risk. Integrating the organizational and cultural dimension into risk management strategies contributes to creating a climate conducive to risk awareness and control, especially in sensitive areas such as cybersecurity. The inability of human resources to correctly identify and assess risks, both internal and external to the organization, can lead to an increase in the level of tolerance towards risk (Kioskli et al., 2025).

This distortion in the perception of risk determines the underestimation of the probability of occurrence of undesirable events and their potential impact, favouring, consequently, the manifestation of risky behaviours in the performance of professional activities. When risks are not correctly understood or are perceived as minor or unlikely, employees may adopt decisions and actions that contradict safety procedures, organizational norms or good professional practices. In the absence of adequate awareness of risks, increased tolerance towards uncertainty becomes a facilitating factor for uncontrolled risk taking, which can amplify organizational vulnerabilities and generate significant negative effects on performance, security and business continuity (Alenzi & Rusho, 2024).

According to Giansanti (2021), the delayed attention to cybersecurity in healthcare in several countries, compared to the United States, is partly explained by differences in how healthcare is conceptualized, as an industry versus a public service. With the exponential growth of innovative, network-connected medical technologies, now exceeding hundreds of thousands of device classes, cybersecurity risks are increasingly intertwined with the safety, effectiveness, and reliability of healthcare delivery, as well as with the protection of sensitive health data. In this context, healthcare cybersecurity encompasses a broad set of measures, including network, application, and information security, operational resilience, disaster

recovery, and end-user training, all adapted to the specific requirements of complex medical devices and interoperable healthcare information systems (Kioskli et al., 2023)

In this context, the development of human resources competencies in the field of risk identification and management becomes essential for reducing risky behaviours and for strengthening an organizational culture oriented towards prevention and responsibility, especially in environments characterized by high complexity and increased exposure to risks, such as cyber.

2. Methodology

The investigative approach aims to highlight the extent to which human resources have the necessary competencies to identify, prevent and manage cyber threats, in an organizational context characterized by accelerated digitalization and increasingly complex technological vulnerabilities. In accordance with the educational standards, the competency system under analysis is structured into six distinct categories, which reflect both the general requirements of professional activity and the specific requirements of the cybersecurity field. These include mandatory competencies, general competencies, economic competencies, competencies in the field of information and communication technologies (IT&C), security ethics competencies, as well as competencies specific to cybersecurity. The integrated approach of these categories of competencies allows for a complex analysis of the human resource capacity to adequately respond to cyber risks, highlighting the interdependencies between basic and specialized competencies. In this sense, the research contributes to the substantiation of clear directions for professional development and continuous training, essential for strengthening organizational resilience and supporting effective cyber risk management.

In line with the general purpose of the study, a series of research objectives were formulated to ensure the identification and analysis of relevant information to substantiate the scientific approach. These objectives are intended to guide the research process and facilitate a systematic assessment of human resource competencies in the context of cyber risk management at the organizational level. The research objectives are the following:

O1: Identification of the current level of competencies of contractual personnel within medical units, in order to assess their level of preparation for managing cyber risks;

O2: Analysis of the competency system, by highlighting the structure, coherence and interdependencies between the categories of competencies analysed;

O3: Detailed analysis of each competency component of the system, in order to determine their specific role and impact in the cyber risk management process;

O4: Understanding the correlation relationships between competencies, as well as how they influence each other within an integrated risk management model.

After defining the objectives that underpinned the scientific research approach, the research plan was developed, structured in the following successive stages:

- Stage 1: Delimitation of the research population: this was made up of contractual personnel who carry out their activity in medical units in Romania. These included both public and private health units, namely hospitals, polyclinics, medical offices and pharmacies.

- Stage 2: Establishing the survey unit: the observation unit was represented by the people who provide services within the medical units and who provided relevant information regarding the level of skills held, as well as the skills needed to carry out the professional activity.
- Stage 3: Designing the questionnaire: the main instrument used in the research was the questionnaire, through which the opinion of the contractual personnel from the medical units included in the sample was investigated. Its development was based on the established objectives of the research, which is why closed questions were mainly formulated, measured on interval or metric scales, intended to capture the level of each analysed competency. For this purpose, a 5-point Likert scale was used, where the value 1 corresponds to a very low level of competency, and the value 5 indicates a very high level.
- Stage 4: Choice of sampling method: the simple random sampling method was applied, the selection of respondents being based on two main criteria, namely their availability and accessibility.
- Stage 5: Exploratory quantitative analysis: data collection took place between August 2021 and November 2021, using the questionnaire as a structured quantitative research instrument, the average time required to complete it being approximately 20 minutes. In the data processing and analysis stage, the SPSS (Statistical Package for the Social Sciences) software package was used, through which descriptive statistical indicators (mean, median, mode) were calculated, multiple linear regression analyses were performed, as well as graphical representations and various data filtering procedures.

3. Results and Discussions

Following the data processing and analysis process, carried out using the SPSS statistical program, and based on the values of the central tendency statistical indicators (mean, median and mode), the following findings can be formulated. Mandatory competencies (62.5%) and general competencies (57%) are implemented at a high level within the analysed medical units, which indicates the existence of a solid framework of basic competencies at the human resource level. Regarding economic competencies, these are assimilated by the human resource at an average level (33%), suggesting a moderate need for consolidation and development in this area. Competencies in the field of information and communication technologies (IT&C) (35.7%), as well as security ethics competencies (33.5%), register a relatively high level of implementation, reflecting an increased concern for the use of digital technologies and for respecting the ethical principles associated with information security.

The analysis of the distribution on the Very Low – Low – Medium – High – Very High rating scale indicates that, in the case of cybersecurity skills, the largest share of respondents (42.7%) falls into the "Low" level, which reflects a low level of possession of these skills at the human resources level. This situation highlights the existence of significant vulnerabilities in the organizational capacities for the effective prevention, detection and management of cyber risks. This situation highlights the need to develop specific cybersecurity training and education programs, adapted to the particularities of the medical sector. The detailed results of the analysis are presented in Table 1.

Table 1: Descriptive statistics of human resource competencies

Competencies						
	Mandatory	General	Economic	I.T. & C	Security Ethics	Cybersecurity
Mean	4.98	4.96	2.70	3.58	3.41	2,65
Median	5.00	5.00	3.00	4.00	3.00	3,00
Mode	5	5	3	4	3	2
Very low	0 %	1 %	9.0%	3.8 %	7.7 %	3.9 %
Low	1 %	1.9 %	12	11.5 %	10.6 %	**42.7 %**
Medium	4.8 %	8.6 %	**33%**	28.8 %	33.7 %	37.9 %
High	31.7 %	31.5 %	14%	**35.7 %**	**33.5 %**	8.7 %
Very high	**62.5 %**	**57 %**	4%	20.2 %	12.5 %	6.8 %

Source: processing data obtained through SPSS program

To investigate the relationships between the different classes of human resource competencies and the level of cybersecurity competencies, the multiple linear regression method was used, with cybersecurity performance as the dependent variable. The independent variables were represented by the average scores corresponding to the analysed competency classes, which are considered predictors of the level of cybersecurity performance. The application of this statistical model aimed to identify those of the analysed competencies that contribute significantly to explaining the variation in cybersecurity competencies, as well as to quantify the influence exerted by each predictor in particular. In the first stage of the analysis, all competency classes identified within the analysed system were introduced into the regression equation, namely mandatory competencies, general competencies, economic competencies, IT&C competencies and security ethics competencies. The results obtained highlighted the fact that only three of these competency classes have a significant predictive role on cybersecurity performance. Thus, information and communication technology (IT&C) competencies, security ethics competencies and economic competencies were found to be relevant predictors, exerting a significant influence on the level of cybersecurity competencies. These results suggest that the level of digital literacy, understanding of ethical principles associated with information security and the ability to assess the economic implications of cybersecurity risks are determining factors in the development of specific cybersecurity competencies. In contrast, mandatory competencies and general competencies did not have a statistically significant influence on cybersecurity competencies, indicating that these, although essential for the performance of current professional activity, are not sufficient to support the development of specialized competencies necessary for managing cyber risks. The lack of a significant predictive effect of these competencies suggests the need for training programs explicitly oriented towards technical, ethical and economic competencies associated with cybersecurity. Overall, the multiple linear regression results confirm the hypothesis that cybersecurity performance is predominantly influenced by specialized competencies, rather than general or mandatory competencies, underlining the importance of a differentiated approach to human resource development. These findings provide empirical support for the substantiation of professional training strategies and organizational policies aimed at strengthening key competencies necessary for increasing cyber resilience at the organizational level.

In the second stage of the analysis, multiple linear regression models were rerun to examine whether variables that were not directly predictive of cybersecurity competencies, namely mandatory competencies and general competencies, can play a significant role in explaining the variation in other relevant competency categories. More specifically, the analysis aimed to determine whether these competencies exert an influence on cybersecurity competencies indirectly, through IT&C competencies, economic competencies and security ethics competencies. In other words, the hypothesis of the existence of a mediation mechanism was tested, in which mandatory and general competencies influence cybersecurity performance not directly, but through the impact they have on the development of intermediate, more specialized competencies. This approach allows for a more nuanced understanding of the relationships between competencies and highlights the role of fundamental competencies as a basis for the formation of advanced competencies. The results of multiple linear regressions indicate the possibility of configuring three distinct predictive models, each based on a different combination of skill classes. The first model uses security ethics competencies as a single predictor, explaining 37.6% of the variation in performance in cybersecurity competencies, which highlights the importance of respecting ethical principles and responsible behaviour in managing information security. The second model extends the structure of the first by including IT&C competencies as an additional predictor. This addition leads to a significant improvement in the predictive capacity of the model, by 10.9% ($p < 0.001$), highlighting the essential role of digital and technical competencies in strengthening cybersecurity at the organizational level.

In the third model, economic competencies are added to the previous predictors, resulting in an explanatory model that manages to explain almost 50% of the variation in performance in cybersecurity competencies. This result highlights that understanding the economic implications of cyber risks and the ability to assess the costs and benefits of security measures contribute significantly to the development of cybersecurity competencies (Table 2).

Table 2: Multiple regression models for predicting cybersecurity competencies

Model	R	R squared	Adjusted R squared	Standard error of estimate	Change statistics				
					R squared modification	Change F	df1	df2	Change meaning F
1	,615[a]	,378	,376	,719	,378	188,385	1	310	,000
2	,698[b]	,487	,484	,654	,109	65,949	1	309	,000
3	,708[c]	,501	,496	,646	,014	8,517	1	308	,004

Note: a. Predictor: (Constant), Security Ethics Competencies; b. Predictor: (Constant), Security Ethics Competencies, IT&C Competencies; c. Predictor: (Constant), Security Ethics Competencies, IT&C Competencies, Economic Competencies

Source: Processing data obtained through SPSS program

In the process of building predictive models, mandatory competencies and general competencies were excluded from the final regression equations, as their associated performances did not generate statistically significant improvements in the prediction of cybersecurity competencies. This reinforces the conclusion that the influence of these competencies is indirect, manifested through their supporting role in the development of specialized competencies, and not through a direct impact on cybersecurity. Overall, these results support the idea of the existence of a hierarchical structure of competencies, in which

fundamental competencies create the necessary premises for the development of intermediate and advanced competencies, with a direct effect on cybersecurity performance.

Conclusion

From a theoretical point of view, the research provides an in-depth perspective on how human resource competencies within medical units are perceived, in relation to the need to manage risks at both the organizational and cyber levels. The study contributes to expanding the existing conceptual framework by integrating the competency dimension into the analysis of risk management, going beyond traditional approaches that treat risk exclusively from a technical or procedural perspective. In the specialized literature, risk management is frequently analysed through the lens of tools, standards and control mechanisms, while the active role of human resources and their competencies remains insufficiently explored, especially in the context of the medical sector. Therefore, this research makes a relevant theoretical contribution by focusing on employees' perceptions of their own competencies and on how they influence organizations' ability to identify, assess and manage risks. A distinctive element of the theoretical approach is the analysis of competencies as an integrated system, structured on several interdependent classes, which reflect both the fundamental and specialized competencies necessary for managing cyber risks. This approach allows for a more nuanced understanding of the relationship between general, technical and ethical competencies, highlighting the fact that performance in the field of cybersecurity is the result of a complex combination of competency factors and not a single isolated dimension.

The research also contributes to clarifying the relationship between the subjective perception of competencies and the real level of training of the human resource, highlighting possible discrepancies between the declared competencies and those effectively required for managing organizational and cyber risks. This theoretical perspective is particularly relevant for the medical field, characterized by a high degree of operational complexity, intensive use of digital technologies and increased exposure to informational risks. At the same time, the study contributes to the consolidation of the specialized literature by highlighting the role of intermediate competencies, such as IT&C, economic and security ethics, as key elements in the process of developing cybersecurity competencies. From this perspective, the research supports the thesis that fundamental competencies create the necessary premises for the formation of specialized competencies, but are not sufficient, in the absence of specific training oriented towards cyber risks. Overall, the theoretical contribution of the research consists in the development of an integrative conceptual framework, which correlates human resource perceptions, the structure of competencies and risk management in a sensitive and insufficiently explored field, such as that of medical units. This approach provides the necessary premises for the further development of theoretical and empirical models regarding the role of human resource competencies in strengthening organizational resilience and cybersecurity.

From a practical point of view, the results obtained in this research provide relevant benchmarks for assessing the capacity of human resources to integrate theoretical knowledge with practical competencies in the process of perceiving and managing cyber risk. The analysis highlights how employees in medical units manage to correlate the information acquired through professional training with practical experience and with their own cognitive competencies, such as critical thinking, the ability to synthesize and analyse complex situations, in order to fulfil the responsibilities provided in the job description. In an

organizational context marked by accelerated digitalization and increased exposure to cyber threats, the capacity of human resources to correctly interpret risks, to anticipate potential vulnerabilities and to adopt appropriate preventive behaviours becomes a determining factor of organizational performance.

The research results suggest that the effective integration of theoretical knowledge with practical competencies contributes to improving the quality of the activities carried out and reducing the likelihood of cybersecurity incidents. At the same time, the study highlights the importance of developing specialized competencies in the field of cybersecurity, as an integral part of the professional competencies of the contemporary employee in the medical sector. The ability to use digital tools safely, to respect the ethical principles of information security and to understand the economic implications of cyber risks directly influences the qualitative level of the results obtained in the professional activity. From a managerial perspective, the research results can constitute support for the development of training and professional development policies aimed at strengthening the competencies necessary for managing cyber risks. The integration of these competencies in job descriptions, in continuous training programs and in performance evaluation systems can contribute to increasing organizational efficiency and ensuring a high level of quality and safety of medical services.

Overall, the practical implications of the research emphasize the central role of human resources in managing cyber risks and highlight the need for an integrated approach, which capitalizes on both the cognitive and applicative dimensions of professional competencies, in order to achieve superior results from a qualitative and operational point of view.

In addition to the theoretical and practical implications highlighted, the research results allow us to outline relevant legal implications generated by the inability of human resources departments to adequately manage cyber risks. In the context of the healthcare sector, where the volume and sensitivity of the processed data are significantly higher, human resource competence deficiencies can lead to serious violations of the applicable legal framework, in particular Regulation (EU) 2016/679 on the protection of personal data (GDPR). The lack of specific skills in the field of cybersecurity and security ethics can generate situations of legal non-compliance, such as unauthorized access to medical data, accidental disclosure of sensitive information or improper use of IT systems. Such incidents can attract legal liability of the organization, including significant administrative sanctions, obligations to notify supervisory authorities and data subjects, as well as potential civil litigation regarding damages caused to patients.

From the perspective of labour law and organizational responsibility law, the results of the study suggest that the failure to integrate cybersecurity skills into job descriptions, training programs and internal procedures can be interpreted as a managerial deficiency in fulfilling legal obligations to ensure data security and a work environment in accordance with the regulations in force. In this sense, the human resources department can no longer be viewed exclusively as an administrative actor, but as a key element in the architecture of legal compliance and governance of cyber risks.

Therefore, strengthening human resource skills in the field of cybersecurity acquires not only an operational and managerial value, but also a legal one, directly contributing to reducing the risks of non-compliance, protecting the rights of data subjects and limiting the exposure of healthcare organizations to legal and reputational sanctions. The integration of the legal

dimension into human resource training and skills assessment policies is thus emerging as a necessary direction for future research and responsible organizational practices.

Credit Authorship Contribution Statement:

Riza, I. was responsible for conceptualization, methodology, data analysis, and manuscript drafting. Bogdan, A. M. contributed to the literature review, data preparation, and visualization. Riza, I., as corresponding author, oversaw validation and communication throughout the review and publication process.

Conflict of Interest Statement

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Acknowledgment

This research was funded by Spiru Haret University, Central Research Institute through Internal Research Grant Program “Challenges in a Technology & Data-Driven Society” (Grant ID 840/13.04.2023), period: 1st May, 2023 – 30th December, 2025.

Data Availability Statement

Data available on request: The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Alenzi, M.A.S., & Rusho, M.A. (2024). A Field Study on the Impact of the Level of Knowledge of Human Resources Employees About the Principles and Applications of Cybersecurity on Human Resources Laws, Between the Theoretical Aspect and the Practical Application Reality. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(21s), 3214–3220. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6011

Chodyka, M., Ciekanowski, Z., Kuznetsov, V., Zurawski, S., Chrzaszcz, A., & Drapikowska, B. (2025). The Role of Human Resource Management in Building an Organisational Security System, Including Cybersecurity, in the Era of Globalisation. *European Research Studies Journal*, Volume XXVIII, Issue 4, 1458-1470. https://doi.org/10.35808/ersj/4192

Dawson, J. (2018). The future cybersecurity workforce: Going beyond technical competencies. *Frontiers in Psychology, 9*, 744. https://doi.org/10.3389/fpsyg.2018.00744

Drozdowski, G., Rogozińska-Mitrut, J., & Stasiak, J. (2021). The empirical analysis of the core competencies of the company’s resource management risk: Preliminary study. *Risks, 9*(6), 107. https://doi.org/10.3390/risks9060107

Regulation (EU) 2016/679 on the protection of personal data (GDPR). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Almada, M. (2025). Training curriculum on AI and data protection Law & Compliance in AI Security & Data Protection. https://www.edpb.europa.eu/system/files/2025-06/spe-training-on-ai-and-data-protection-legal_en.pdf

Giansanti, D. (2021). Cybersecurity and the Digital-Health: The Challenge of This Millennium. *Healthcare*, *9*(1), 62. https://doi.org/10.3390/healthcare9010062

Kioskli, K., Seralidou, E., & Polemi, N. (2025). A practical human-centric risk management approach integrating HRM tools for cybersecurity. *Electronics, 14*, 486. https://doi.org/10.3390/electronics14030486

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. *Applied Sciences*, *13*(6), 3410. https://doi.org/10.3390/app13063410

Nurse, J.R.C., Milward, J., Alashe, O. (2025). From Security Awareness and Training to Human Risk Management in Cybersecurity. In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2025. *Lecture Notes in Computer Science,* Volume 15814. Springer, Cham. https://doi.org/10.1007/978-3-031-92833-8_6

Sayvaya, I., & Siagian, M. V. (2024). Cybersecurity awareness as a component of HR policies: Protecting employee and organizational data in the digital era. *Ambidextrous Journal, 2*(2), 187. https://doi.org/10.61536/ambidextrous.v2i02.187

Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy*, Volume 46, Issue 3, 102282. https://doi.org/10.1016/j.telpol.2021.102282

Zhang, X., Wang, P., & Peng, L. (2024). Developing a Competency Model for Human Resource Directors (HRDs) in Exponential Organizations Undergoing Digital Transformation. *Sustainability*, *16*(23), 10540. https://doi.org/10.3390/su162310540

How to cite this article

Riza, I., & Bogdan, A. M. (2025). Human Resource Competencies in Healthcare Cybersecurity: Risk Management and Legal Compliance Implications. *Applied Journal of Economics, Law and Governance*, Volume I, Issue 2(2), 205-216. https://doi.org/10.57017/ajelg.v1.i2(2).06

Article's history:

Received 25th of November, 2025; Revised 7th of December, 2025;
Accepted for publication 27th of December, 2025; Available online: 30th of December, 2025
Published as article in Volume I, Issue 2(2), 2025