European Research Studies Journal
Volume XXVIII, Issue 4, 2025

pp. 1458-1470

The Role of Human Resource Management in Building an Organisational Security System, Including Cybersecurity, in the Era of Globalisation

Submitted 19/10/25, 1st revision 04/11/25, 2nd revision 16/11/25, accepted 10/12/25

Marta Chodyka[1], Zbigniew Ciekanowski[2], Valeriy Kuznetsov[3], Sławomir Żurawski[4], Aneta Chrząszcz[5], Barbara Drapikowska[6]

Abstract:

Purpose: *The purpose of the article is to highlight the strategic role of human resource management (HRM) in building organisational security and resilience, with particular emphasis on cybersecurity and information security systems in the context of globalisation. In particular, the analysis focuses on how HRM functions and tools, such as employee selection, competence development, security culture, knowledge management, and employee well-being, contribute to reducing the vulnerability of organisations to threats—including cyber threats and information security breaches—and strengthening their adaptability and crisis response capabilities.*

Design/methodology/approach: *The article uses a critical analysis of scientific literature in the field of strategic human resource management, organisational resilience, and risk management. The study is also based on a comparative analysis of data and findings from international and industry reports, as well as reports on the labour market, competencies, and digital transformation. The research problem is formulated as follows: To what extent does strategic human resource management affect the security and resilience of organisations, including information security and cybersecurity, operating in conditions of global threats? The research hypothesis posits that organisations that integrate human resource management with their security and risk management systems will achieve a higher level of resilience, operational stability, and effectiveness in responding to threats. The research approach involves comparing theoretical findings and reports on organisational behaviour during crises, which has enabled the development of a conceptual model indicating the relationships between HRM and organisational security.*

[1]*John Paul II University in Biala Podlaska, Poland, ORCID: 0000-0002-8819-2451*
e-mail: m.chodyka@dyd.akademiabialska.pl*;*
[2]*War Studies University, ORCID: 0000-0002-0549-894X, e-mail:* zbigniew@ciekanowski.pl*;*
[3]*Railway Research Institute, ORCID: 0000-0003-4165-1056,*
e-mail: valeriy.kuznetsov@mans.org.pl*;*
[4]*State Academy of Applied Sciences in Chełm, Poland, ORCID: 0000-0001-9527-3391,*
e-mail: slawomir.zurawski@onet.pl*;*
[5]*John Paul II Academy in Biała Podlaska, Poland, ORCID: 0000-0001-9749-274X,*
e-mail: aneta.chrzaszcz@op.pl*;*
[6]*War Studies University, ORCID 0000-0002-6852-2791, e-mail:* bdrapikowska@o2.pl*;*

Findings: *The results indicate that strategic HRM is a key factor in determining organisational security. The effective integration of HR tools, particularly in areas such as selection, competence development, safety culture, knowledge management, and well-being, enhances the organisation's adaptability, minimises risks associated with human error, and strengthens its preparedness for both external and internal disruptions.*
Practical implications: *a catalogue of practical HR tools supporting security is presented, including security-oriented training systems, in information security and cybersecurity (e.g., cyber hygiene training, phishing simulations), background screening, competency models, personnel risk assessment and monitoring systems, as well as well-being programmes that reduce the risk of errors resulting from employee stress and overload.*
Original value: *The article contributes to both theoretical and practical value by presenting a coherent model for integrating HRM with organisational security and resilience systems. It also emphasises the importance of international reports and research on global threats as a basis for assessing the role of HR in maintaining the stability of modern organisations.*

Keywords: *Human resource management, organisational security, cybersecurity, organisational resilience, risk management.*

JEL codes: *M12, J24, M14, M15.*

Paper type: *Research article.*

1. Introduction

Dynamic globalisation processes, the development of information technologies, the growing complexity of markets, and intense international exchange mean that contemporary organisations operate in an environment characterised by a high level of uncertainty and vulnerability to various threats.

Globalisation, while opening up opportunities for faster growth, innovation, and market expansion for organisations, also generates new challenges to their stability and security.

Threats arise not only from external factors such as geopolitical instability, cyberattacks, global competition, and supply chain disruptions, but also from internal factors related to human capital. In this context, the importance of human resource management as a strategic area that determines organisational security is growing.

Contemporary approaches to security recognise people as a key element in both generating and minimising risk. Employees' competencies, attitudes, level of risk awareness, and compliance with procedures directly impact an organisation's ability to maintain business continuity and ensure resilience in the face of incidents.

Therefore, human resource management is no longer an administrative function, but has become one of the most essential pillars of the security system – covering not only recruitment and selection processes, but also building a culture of security, developing training systems, motivating personnel, assessing personnel risk, and strengthening the adaptive competencies of employees.

In the era of globalisation, organisations need employees who are capable of operating in conditions of volatility, pressure, and multidimensional threats. Human resource management is therefore becoming a tool for building both operational security and strategic resilience, allowing organisations to respond to threats in a flexible, coordinated, and responsible manner. This study attempts to analyse the role of HRM as the foundation of organisational security, highlighting its importance in the context of global challenges and practices that strengthen the stability of modern entities.

2. Globalisation and Organisational Security – New Challenges, Threats

The process of globalisation—understood as the intensification of the flow of people, capital, information, and technology—has led to a significant interpenetration of domestic and international affairs, increasing interdependence between entities of social and economic life (Grima *et al.,* 2023).

Globalisation has become one of the key factors in the evolution of the concept of security, blurring the boundaries between national and international security and demilitarising this category in favour of approaches that also cover social, economic, and technological areas (Grzebiela, 2018, p. 89; Tyagi *et al.,* 2023).

Securitology literature emphasises that, in the context of globalisation, security ceases to be merely a state of absence of threats and is increasingly defined as a process of actively shaping the conditions for the survival, development, and protection of an entity's key resources, including organisations (Grzebiela, 2018, p. 95).

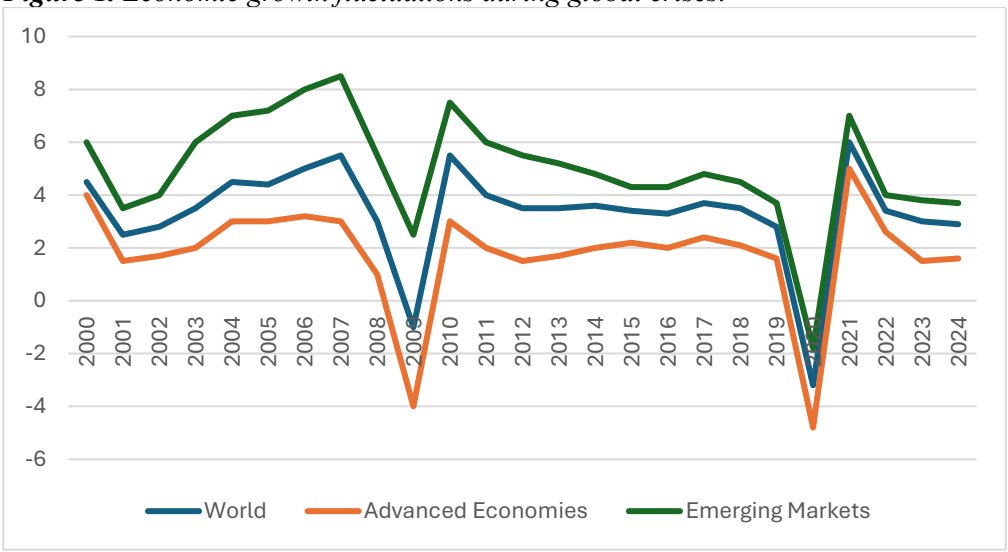
Wałek points out that at the dawn of the 21st century, globalisation has generated a new class of threats that are transnational in nature, difficult to predict, and spreading at an unprecedented speed (Wałek, 2013). The author includes among them phenomena of a socio-economic nature (poverty, unemployment, inequalities), but also terrorism, organised crime, and migration forced by conflicts and crises (Wałek, 2013, p. 70). A characteristic feature of these threats is that they "travel" along global chains of connections – from the international level to the regional and local levels – and thus directly affect the security of specific organisations operating in this environment.

The latest reports on global risk emphasise that we are facing the so-called "era of systemic risk" and "polycrisis" – a multiple, overlapping crisis resulting from the simultaneous materialisation of numerous political, economic, environmental, and technological threats. Contemporary social and economic systems have become so

complex and interconnected that any significant disruption in one area (e.g., energy, public health, cyberspace) can cascade into other sectors (ASRA, Facing Global Risks with Honest Hope, 2024, pp. 9-11).

The authors of the report note that the growing number of crises—from pandemics and armed conflicts to the cost-of-living crisis—means that the classic, "siloed" approach to organisational security management is no longer sufficient. The fluctuations in economic growth during global crises are presented in Figure 1 below.

Figure 1. *Economic growth fluctuations during global crises.*



Source: *ASRA, Facing Global Risks with Honest Hope, 2024, p. 16.*

In an "increasingly interconnected" world, countries, organisations, and societies are exposed to environmental volatility, and threats can arise simultaneously in the technological, economic, social, and information dimensions. In such conditions, organisational resilience becomes a key concept, understood in accordance with BS 65000 as the ability of an organisation to anticipate changes and disruptions, prepare for them, respond to them, and adapt to survive and continue to develop (British Standard BS 65000: Organisational Resilience, 2014).

Companies must continually face the challenges posed by ongoing changes and unforeseen situations that impact the continuity of the organisation's operations. The response to such changes should be a four-stage process:

- The first stage, which should initiate the process, should be the acceptance of the occurrence of changes and their possible adverse effects on production capacity;

- Thanks to this awareness, the company should ensure the continuity of its operations (stage two), regardless of the form of disruption and possible limitations to the efficiency and functionality of processes;
- The company should focus on returning to the neutral position it was in before events that slowed down the company's operations – stage three;
  The final stage of the process involves using the experience gained from the previous steps to strengthen the organisation's resilience through proactive analysis of events and lessons learned.
  https://www.organisationalresilience.gov.au.

British Standards Institution BSI analyses confirm that in recent years there has been a decline in the overall assessment of organisational resilience in the areas of leadership, people, processes, and products, despite the simultaneous improvement in the financial results of many companies. The study indicates, among other things, that in some economies (e.g., Japan, the United Kingdom, and Ireland), a significant percentage of companies reported a deterioration in financial performance, even though globally, most entities reported an improvement.

There is an important "perception gap" between how leaders assess the importance of individual resilience factors (e.g., adaptability, horizon scanning) and how they evaluate the actual effectiveness of their own organisations in these areas (BSI Organisational Resilience Index Report 2021). This indicates that the global risk environment is outpacing the ability of many organisations to respond and adapt, which directly impacts their level of security.

The digital dimension of globalisation has a particularly significant impact on the security of organisations. The development of information and communication technologies, the digitisation of services, and the rise of remote work and collaboration have created a new infrastructure for the operation of businesses, governments, and public institutions.

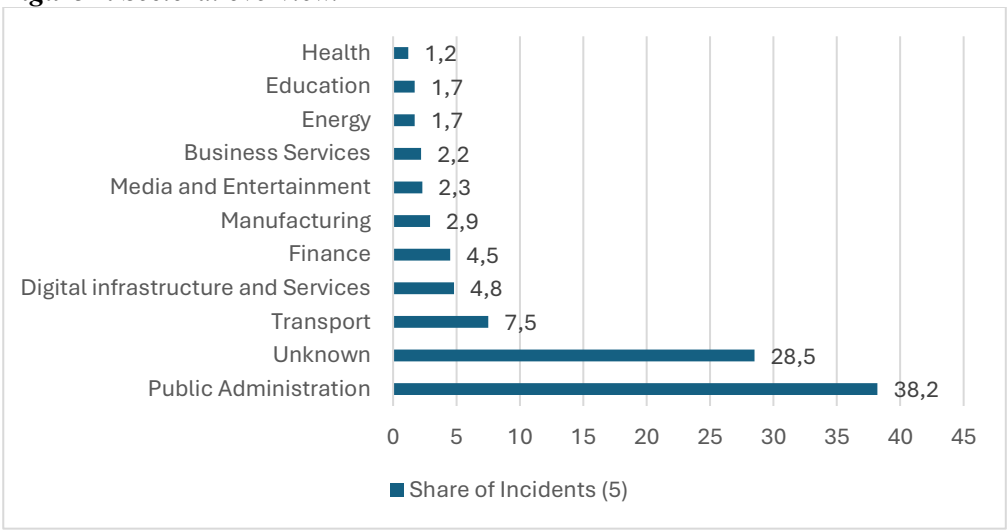
Public organisations have become integral to the information society, where the security of the information system not only determines the entity's efficiency but also impacts the broader security of the state. At the same time, low awareness of threats among users, organisational errors, and the rapid pace of technological development mean that the gap between the actual level of risk and the ability to control it is steadily widening.

The number of incidents broken down by sector is presented below (Figure 2). This means that cybersecurity should be treated not only as the domain of IT departments, but as a key component of the organisational security system, closely linked to human resource management policies and practices.

The particularly vulnerable sectors were public administration, transport, digital infrastructure, and finance—areas that are key to the continuity of the state and the

economy. European Union Agency for Cybersecurity (ENISA) also points out that attacks on supply chains are becoming increasingly important, and threat actors are increasingly using employees (especially those with elevated privileges) as a "gateway" into organisations, which directly links the technical dimension with the human factor.

Figure 2. *Sectoral overview.*



Source: *ENISA Threat Landscape 2025.*

The literature on business security emphasises that the scale and complexity of contemporary threats necessitate a shift from a traditional, reactive approach to security toward concepts based on proactivity, resilience, and risk management at the organisational level.

Chodyński, analyzing business security in conditions of global turbulence (pandemics, natural disasters, armed conflicts, energy crises), points out that corporate security is today becoming a strategic category, closely linked to its competitiveness and ability to survive (Chodyński, 2023, pp. 6-8). This means that organisational security cannot be treated as a narrow domain of security services or the IT department, but rather as an integrated system encompassing structure, processes, organisational culture, and, as will be discussed in subsequent parts of this article, human resource management.

Globalisation has increased the exposure of organisations to complex, interrelated systemic threats, particularly digital and information risks. Data from international reports and research on organisational resilience indicate that many entities are still lagging in adapting their security systems to the evolving dynamics of the environment.

In such conditions, the importance of internal factors is growing, especially the quality of human resource management, which determines whether an organisation can accurately identify threats, design adequate protective mechanisms, and consistently implement them. It is precisely the role of HRM in building an organisation's security system that will be the focus of the following parts of this study.

3. Human Resource Management is the Foundation of Organisational Security

Human resource management (HRM) today plays a role that goes far beyond traditional HR functions. HRM is a comprehensive process that includes employment planning, recruitment, selection, adaptation, development, motivation, evaluation, and shaping the organisational culture (Wicińska, 2021, p. 15). Modern HRM concepts view employees not as a cost, but as a strategic resource of the organisation, representing human capital that can determine a competitive advantage, adaptability, and sustainability (Mikuła, Myjak, and Trzcińska, 2023).

In the context of organisational security, human resources are both a significant source of risk and a crucial element in ensuring the stability and resilience of an entity. The high effectiveness of an organisational security system largely depends on HR activities, including the selection, development, motivation, and management of human resource diversity (Ciekanowski *et al.,* 2023, p. 808). HRM enables the identification, assessment, and management of personnel risks, including errors, negligence, and potential deliberate actions ("insider threats") (Nica *et al.,* 2024).

Proper recruitment and selection can reduce the likelihood of hiring people who are unsuitable in terms of competence, ethics, or credibility. The literature on information system security emphasises that HR plays a key role in protecting information resources, including conducting background checks, providing IT security training, granting and monitoring access rights, and continually raising security awareness among employees (Guo, 2024). From a cybersecurity perspective, HRM practices therefore constitute a "soft layer" of protection, determining the effectiveness of technical and procedural solutions.

Based on a review of the literature, the main HR functions that directly support organisational security can be identified:

1. Recruitment and selection: Selecting employees with the right skills, aptitudes, values, and ethics as the first line of defence against internal risk.
2. Training and competence development (including security): Continuous improvement of qualifications, education in security procedures, information protection, and cyber hygiene. Such practices significantly reduce the number of incidents resulting from ignorance or errors.

3. Motivation and engagement management: Loyal, appreciated, and engaged employees are less likely to take risky actions, are more responsible, and are more aware of the need to follow safety rules.
4. Shaping organisational culture and internal communication: In organisations that promote the values of safety, responsibility, and transparency, it is easier to report incidents, follow procedures, and cooperate in a crisis.
5. Personnel risk management: HR can act as part of the risk management system—identifying, monitoring, and minimising personnel-related risks, such as turnover, conflicts, errors, and internal risks (Babkin *et al.,* 2023).

The availability of qualified, well-educated, and experienced employees significantly improves a company's ability to manage risk and achieve stable results. HRM is increasingly seen as a strategic function — integral to the mission, strategy, and risk management system of an organisation. In this context, personnel policy is not just a human resources operation, but a tool for building organisational resilience and long-term stability (Becker and Smidt, 2016).

A human resource management model that integrates HR activities with security policy, from selection and training to monitoring and communication, is becoming a crucial component of an organisation's security system, alongside procedures, technology, control systems, and risk management.

Human resources can be considered not only in terms of competencies, but also in terms of their demographic diversity, experience, work style, perspectives, and attitudes. This diversity increases the organisation's potential for adaptation, innovation, and response to various types of threats. In the context of security, this can be an advantage: the broader the set of experiences and skills, the easier it is for the organisation to anticipate, identify, and neutralise threats.

Human resource management is the foundation for building organisational security (Ciekanowski *et al.,* 2025). Through a comprehensive approach that encompasses selection, development, motivation, organisational culture, training, and personnel risk management, HR becomes a vital element of the protection and resilience system. In an environment of growing threats, uncertainty, and complexity, the quality of personnel policy, competencies, and employee awareness can determine whether an organisation will withstand crises or fall victim to them.

4. Human Resource Management Tools and Practices that Strengthen the Security and Resilience of an Organisation

Contemporary organisations operate in a highly volatile environment, which requires the implementation of integrated HR tools that strengthen security and structural and operational resilience.

These tools are not limited to personnel issues, but include training systems, recruitment procedures, competency management, assessment systems, safety culture, knowledge management, employee well-being, and safety-supporting technologies.

From the perspective of building a cybersecurity system, HR practices that aim to reduce human risk are critical. These include, among others, systematic training in information security and cyber hygiene (phishing recognition, password creation rules, secure remote working), procedures for verifying candidates and employees in positions with increased access privileges (background screening), clear rules for granting, changing, and revoking access to IT systems, as well as programs for building a cybersecurity culture that encourages the reporting of incidents and irregularities.

Another critical area is monitoring personnel risk in the context of insider threats, which requires close cooperation between HR, security, and IT departments (Nica *et al.,* 2024; Guo, 2024).

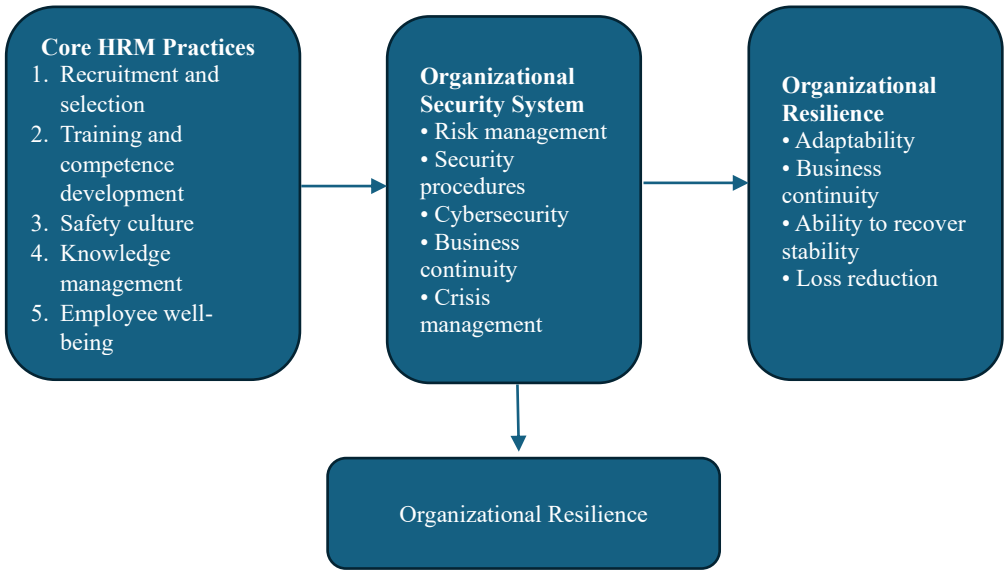
Research indicates that strategic human resource management (HRM) significantly enhances organisational resilience through flexibility, leadership, effective resource planning, and effective management of organisational culture. In one of the latest holistic studies, the authors conclude that SHRM practices (flexible HR, agile leadership, and resource planning) increase an organisation's ability to adapt in times of crisis (Widowati and Damiyana, 2025).

Similarly, a widely cited empirical study of Chinese companies has shown that SHRM has a significant positive impact on organisational resilience, both directly and through an increase in employees' self-efficacy (Yu *et al.,* 2022). For this reason, HR strategies, and not just operational procedures, should be treated as a key component of an organisation's security system.

Human resource development (training, improvement, career development, competencies) has long been considered a fundamental element of building organisational advantage. In the Polish context, work on human resource development shows that investment in employees (their skills, development, adaptation) translates into the organisation's ability to survive and adapt to change (Grzesik and Szkwarek, 2015, p. 1090).

What is more, competency management (a competency-based approach to HR) helps to match the employee's profile to the organisation's requirements, which minimises the risk of errors, wrong decisions, or competency gaps that may pose a threat to security. The model of HR integration and organisational resilience is presented in Figure 3 below.

Figure 3. *Model of integration of HRM practices, organisational security system (including cybersecurity), and organisational resilience.*



Source: *Own work.*

In a dynamic environment of change, crises, and uncertainty, HR flexibility (flexible workforce planning, variable forms of work, staff adaptability) is essential. A 2025 study reveals that a flexible approach to HR, agile personnel management, and adaptation to changing conditions enhance organisational resilience (Widowati and Damiyana, 2025).

At the same time, organisational culture, defined as a set of values, norms, and practices that mediate between SHRM and organisational resilience, proves to be crucial. A 2024 study found that a well-organised culture significantly enhances resilience (Georgescu *et al.,* 2024). This makes organisations more resistant to disruptions, able to adapt more quickly to change, and respond more effectively in crises.

In the practice of managing a modern organisation, HR cannot be treated as a separate operational function. It should be an integral part of the strategy and risk management system. As the authors of an analysis of publicly traded companies point out, if HR strategy is flexible and consistent with the company's strategy, it builds organisational resilience. It enables survival in conditions of regression or progress (Kołodziej, 2024).

In particular, effective resource planning, training, competency management, and fostering a culture that promotes engagement and resilience can minimise the effects

of crises (including people, processes, and external threats) and provide real protection against organisational destabilisation.

5. Summary

In the era of globalisation, organisational security is becoming one of the key conditions for stable functioning and long-term development. The changing geopolitical environment, the growing complexity of the economy, the rapid pace of technological progress, the digitisation of processes, and the increasing interdependence of markets mean that modern organisations are exposed to a wide range of threats, both external and internal.

The analysis conducted in the article clearly indicates that a key element in strengthening organisational security and resilience is human resource management—no longer just a personnel function, but a strategic area that shapes the organisation's ability to adapt, respond, and anticipate.

The analysis showed that globalisation not only increases the number of threats, but also changes their nature – they become more dynamic, difficult to predict, and strongly interrelated. In such an environment, it is people, their competencies, awareness of threats, and ability to learn and act under stress that form the foundation for the effective functioning of the security system.

Human resource management, based on a coherent strategy, appropriate selection of candidates, competence development, building a safety culture, and personnel risk management, becomes a key factor in reducing an organisation's vulnerability to threats.

The article demonstrates that HR tools, including training systems, competency-based job models, employee selection and verification procedures, appraisal systems, knowledge management, and the development of a safety culture, have a direct impact on an organisation's resilience.

A strategic approach to HRM, in which human resources are treated as part of the risk management system and as a key factor in stability, is particularly important. Organisations that integrate HR activities with their security policy and operating strategy are better able to cope with crises, recover more quickly from disruptions, and are more adaptable.

The analysis clearly indicates that organisational security in the context of globalisation requires a departure from an approach based solely on technical or procedural protection measures. It is essential to invest in human capital through competence development, fostering a security culture, promoting employee well-being, creating conscious and flexible work structures, and engaging employees in

decision-making processes. It is people, their attitudes, knowledge, and readiness to act that constitute a fundamental safeguard for the organisation against threats.

In summary, the effectiveness of an organisation's security system largely depends on the quality of human resource management. Organisations that treat HR as a strategic element of security, develop staff competencies, and create a culture based on trust, responsibility, and risk awareness achieve a significantly higher level of resilience, stability, and survivability in uncertain conditions.

Modern human resource management is therefore becoming not only an administrative area, but also a foundation for the security and sustainable development of an organisation. This is particularly true in the area of cybersecurity, where user errors and negligence are among the primary sources of incidents, and properly designed HR practices (including recruitment, training, incentive systems, and safety culture) are the first line of defence against cyber threats.

When creating a cybersecurity system, organisations should therefore develop a long-term human resource management strategy in parallel with technical solutions, focused on building awareness, responsibility, and resilience among employees.

References:

ASRA, Facing Global Risks with Honest Hope, 2024.

Babkin, I., Pulyaeva, V., Ivanova, I., Veys, Y., Makhmudova, G. 2023. Developing a System for Monitoring Human Resource Risks in a Digital Economy, Risks, 11(5), 1-20.

Becker, K., Smidt, M. 2016. A risk perspective on human resource management: A review and directions for future research, Human Resource Management Review, Volume 26, Issue 2, 149-165.

British Standard BS65000: Organizational Resilience. 2014.

BSI Organisational Resilience Index Report. 2021.

Chodyński, A. 2023. Business security. Management aspects. Introduction, "Security. Theory and Practice", 4(LIII).

Ciekanowski, Z., Nowicka, J., Żurawski, S., Mikosik, P. 2023. Human Resources in Organisational Security Management. European Research Studies Journal, Volume XXVI, Issue 4, pp. 802-812.

Ciekanowski, Z., Rejman, K., Żurawski, S., Kacprzak, M., Sirojc, Z. 2025. Personal Safety in the Management of Contemporary Organizations. European Research Studies Journal, Volume XXVIII, Issue 1, pp. 57-66.

ENISA Threat Landscape. 2025.

Georgescu, I., Bocean, C.G., Vărzaru, A.A., Rotea, C.C., Mangra, M.G., Mangra, G.I. 2024. Enhancing Organizational Resilience: The Transformative Influence of Strategic Human Resource Management Practices and Organizational Culture. Sustainability, 16(10), 4315.

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.
Grzebiela, K. 2018. The Concept and Essence of Information Security. Journal of Modern Science, 4(39).
Grzesik, K., Szkwarek, K. 2015. Human resource development as an element of organisational development. Marketing and Market, No. 5, pp. 1081-1093.
Guo, T. 2024. Human Resource Management in Information Security, Atlantis Highlights in Social Sciences, Education and Humanities. Proceedings of the 2024 5th International Conference on Modern Education and Information Management (ICMEIM 2024), pp. 51-61.
Kołodziej, D. 2024. Human resources strategies and organisational resilience in selected publicly traded companies, Scientific Papers of Silesian University of Technology. Organisation and Management Series, no. 208, pp. 183-196.
Mikuła, B., Myjak, T., Trzcińska, M. 2023. Introduction to human resource management. Functions and instruments, Scientific Publishing House of the Academy of Applied Sciences in Nowy Sącz, Nowy Sącz.
Nica, E., Burcea, Ș.G., Sabie, O.M. 2024. The Critical Role of Human Resources in Mitigating and Managing Cybersecurity Risks in Modern Organisations: A Strategic Approach. Psychosociological Issues in Human Resource Management 12(2), pp. 18-49.
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.
Wałek, T. 2013. Globalisation as the main threat to security in the 21st century, "Securitologia", 2(18).
Wicińska, K. 2021. The essence of human resource management [in:] Human resource management (essence, conditions, components, specificity), eds. I. Żuchowski, A. Chętnik, Scientific Society of Ostrołęka, Ostrołęka.
Widowati, R.D. 2025. Resilience in Human Resource Management: Organisational Adaptation Strategies in the Tourism Industry during Times of Uncertainty and Crisis. Brilliant International Journal of Management and Tourism, 5(2), pp. 236-246.
Yu, J., Yuan, L., Han, G., Li, H., Li, P. 2022. A Study of the Impact of Strategic Human Resource Management on Organisational Resilience, Behav. Sci, 12, 508, pp. 1-18.