

Marko Stanojević*
<https://orcid.org/0009-0007-7241-5503>
Danilo Izgarević**
<https://orcid.org/0009-0000-0785-3055>

UDC: 005.961:005.336.1
005.73:005.934

DOI: 10.5937/MegRev2502105S

Original scientific paper

Received 15.06.2025.

Approved: 17.09.2025.

THE ROLE OF HUMAN RESOURCE MANAGEMENT IN ENHANCING CORPORATE INFORMATION SECURITY CULTURE

Abstract: *Organizations are increasingly wrestling with the task of safeguarding their digital and physical assets, especially as security threats, both from within and outside, grow more complex. While technological solutions are crucial, human behavior remains one of the most significant and vulnerable aspects of corporate security systems. This paper examines the key role of Human Resource Management (HRM) in fostering and bolstering a solid corporate security culture. It examines how various HRM functions, including recruitment, onboarding, employee training, policy enforcement, and performance evaluations, can be effectively leveraged to shape employee behavior, decrease human error, and strengthen the overall resilience of the organization. This paper introduces a novel viewpoint on Human Risk Management, which seeks to identify, assess, and mitigate the vulnerabilities associated with human actions. This includes issues like falling for phishing scams, insider threats, and mishandling data. It specifically addresses the challenges that come with hybrid and remote work environments, where security risks can increase due to the spread of technology and communication hurdles. The paper highlights how essential it is to align security awareness programs with the overall culture and values of the organization. It suggests moving away from the usual compliance-focused training and instead adopting more engaging, behavior-driven approaches.*

Keywords: Human Resource Management, Information Security, Corporate Security, Human Risk, Cybersecurity Awareness

* E-mail: stanojevic.marko799@gmail.com

** E-mail: daniloizgarevic@gmail.com

1. INTRODUCTION

Organizations are tasked with the challenging job of keeping operations running smoothly while also protecting both their physical and intangible assets from various security threats. Human Resource Management (HRM) plays a key role in influencing how employees understand, respond to, and follow security guidelines, which ultimately shapes the overall security culture of the company. This culture consists of the shared values, beliefs, practices, and behaviours that dictate how seriously security is regarded at all levels. Creating a strong security culture is essential for reducing insider threats, ensuring compliance with security policies, and strengthening the organization's overall resilience.

Numerous studies have highlighted that the culture within an organization greatly influences how employees deal with information security. In settings where there's a strong emphasis on internal focus, control, or hierarchy, employees are generally more likely to follow security policies.¹ Additionally, human resource management (HRM) practices, like thorough background checks, continuous security training, performance reviews tied to security outcomes, and monitoring are vital for boosting information systems security.² Studies in similar environments have found a strong link between HR processes and the success of information security measures, underscoring HR's essential role in connecting organizational policies with employee security behaviour.³

Cultural alignment looks to be an essential factor in how effective HRM interventions can be. Studies focusing on organizational culture and information security culture indicate that the broader corporate culture can impact whether specific security subcultures flourish or falter.⁴ When employees connect with common values, it can really enhance information security practices, often bolstered by aspects like psychological capital.⁵ It's interesting to note that while we often talk

¹ Karlsson, M., Karlsson, F., Åström, J. & Denk, T. (2022): "The effect of perceived organizational culture on employees' information security compliance", *Information and Computer Security*, 30(3), 382-401.

² Kumah, P. (2022): "The Role of Human Resource Management in Enhancing Organizational Information Systems Security" in: *Research Anthology on Business Aspects of Cybersecurity* (pp.300-325).

³ Al-Thunaibat, M.Y., Al-shawabkeh, A.A. & Al-baqor, K. K. (2020): "The Role of Human Resource Management Processes in Achieving Information Security: An Applied Study on Saudi Government Universities", *Management & Economics Research Journal*, 2(3), 1-23. DOI: 10.48100/merj.v2i3.107

⁴ Solomon, G., & Brown, I. (2021): "The influence of organisational culture and information security culture on employee compliance behaviour", *Journal of Enterprise Information Management*, 34(4), 1203-1228.

⁵ Riemenschneider, C. K., Burney, L. L & Bina, S. (2023): "The influence of organizational values on employee attitude and information security behavior: The mediating role of

about safety culture in terms of physical health, it actually has a lot in common with security culture. When we look at HRM practices that promote a safety culture, like training, engaging employees, and changing mindsets, we see that these elements are also crucial for building a robust security culture.⁶

Employee interactions with policies, sharing of sensitive information, and interpretation of organisational regulations are all impacted by communication in virtual settings, particularly within legal-informatics systems. A security-oriented culture can be strengthened by reducing uncertainty and the danger of non-compliance through efficient virtual communication channels supported by transparent legal-informatica protocols.⁷ HR must make use of this communication infrastructure in companies where remote or hybrid work is prevalent in order to establish security standards, direct employee conduct, and guarantee responsibility in dispersed environments. According to a 2024 study of IT and security experts, almost 87% of participants were employed by companies that provide quarterly or more training to staff members on how to recognise cyberattacks. Furthermore, 33% of respondents stated that they are afraid about human error and faults in how staff members respond.⁸

While interest in this area is on the rise, we still face significant gaps in understanding how HRM can best design, implement, and uphold a security culture that works across different industries and national settings. The differences in organizational cultures, employee values, and outside regulatory pressures indicate that a “one-size-fits-all” approach to HRM security strategies might not work. Additionally, there’s still a lack of empirical research that clearly outlines how HRM practices lead to tangible improvements in security culture and the resulting security outcomes.

This paper sets out to explore the ways in which certain HRM strategies can improve the security culture within companies. It aims to identify the most effective HRM practices, understand their interaction with organizational culture, and uncover the factors that can either promote or impede their successful implementation.

psychological capital”, *Information and Computer Security*, 31(2), 172-198.

⁶ Al-Mekhlafi, A.-B. A. (2025): “Importance of Effective Human Resources Management in Creating a More Secure Work Environment by Improving Safety Culture”, *International Journal of Intellectual Human Resource Management (IJIHRM)*, 5(01), 14-23.

⁷ Baltezarevic, I. & Baltezarević, R. (2020): „Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku”, *Megatrend Revija*. 17(4), 27-40. DOI: 10.5937/MegRev2004027B

⁸ Petrosyan, A. (2025): *Human risk management in global organizations 2024*, https://www.statista.com/statistics/1622615/human-risk-management-global/?srsltid=AfmBOooug_aRonZEFQYjDazd0Q1vLnuU5Kv6BllQZoyl73Ksc3u46y.

2. LITERATURE REVIEW

Employees at a certain organisation with a range of backgrounds and expertise make up its human resources. In the social sciences, this word refers to the workforce as one of the three means of production; in the economic unit management context, it refers to specific employees and business departments that deal with personnel policy.⁹ On the other hand, human resource management encompasses all aspects of personnel management, including hiring, onboarding, performance reviews, and training. It involves developing a productive workforce that advances organisational objectives. The goal of human risk management is to recognise and reduce the hazards associated with human conduct. These two HRMs have a complimentary relationship. While human risk management makes sure those personnel perform securely, human resource management lays the groundwork by recruiting, educating, and involving staff members.¹⁰ Human Risk Management could identify employees who are more susceptible to phishing attempts and offer more focused training, while Human Resource Management might offer broad security awareness training. Human Risk Management guarantees compliance through frequent audits and feedback loops, whereas Human Resource Management may develop regulations pertaining to data handling.¹¹

The creation of a powerful personal brand and a consistent marketing communication plan show how people's actions, how they portray themselves, and how they internalise their principles can affect how others perceive their professionalism, accountability, and trustworthiness inside a company.¹² Similar dynamics can be used by HRM to reinforce a security culture by motivating staff members to internalise organisational security values and act in ways that consistently reflect those values. Putting a strong emphasis on communication that is honest, aligned with values, and consistent helps minimise the gaps between what individuals do and what organisations demand.

Human risk is the possibility that an individual's activities, whether deliberate or not, and whether coming from within or without, will disrupt or harm an organisation. Human risk, also referred to as human error, is a topic that has

⁹ Pujer, K. (2017): "Zarządzanie rozwojem pracowników. Założenia teoretyczne i praktyczne egzemplifikacje", in: Buzowska, B., Paliga, R., Pujer, K.: *Zarządzanie personelem w organizacji. Wybrane problemy teorii i praktyki*. Wydawnictwo Exante, Wrocław.

¹⁰ Baltezarević, B., Baltezarević, R., & Baltezarević, V. (2018). Aktivnosti starijih osoba na onlajn društvenim mrežama. *Megatrend revija*, 15(3), 167.

¹¹ Robinson, K. (2024): *HRM: The Difference Between Human Risk and Resource Management in Cyber Security*, <https://www.metacompliance.com/blog/cyber-security-awareness/hrm-human-risk-and-resource-management>.

¹² Milovanović, S., Lukinović, M. & Baltezarević, R. (2018): "Lični brend i integrisano market-ing komuniciranje", *Megatrend revija*, 15(1), 177-186. DOI: 10.5937/MegRev1801177M

recently gained attention from the cyber security sector, which is always trying to stay one step ahead of its enemies. Because AI-based security solutions have made it easier and more common to thwart broad attempts, cybercriminals have turned their attention to focused tactics that capitalise on human error. In order to prevent this increasing human risk, organisations must change.¹³ One of the most important issues for businesses is still the protection of HR data. Due to the digital storage of sensitive employee data, such as addresses, banking information, and social security numbers, businesses are finding it more and more difficult to safeguard this information from ever-increasing dangers. HR teams must give strong data security measures top priority in order to reduce risks due to the growth of remote and hybrid work, a changing regulatory environment, and an increase in cyberattacks.¹⁴

It is the duty of all employees and other stakeholders in an organisation to ensure the security of HR data. However, there is a unique and significant responsibility for the human resources department. It should guarantee that every employee receives adequate data protection training. Additionally, they must develop and implement policies that protect all of the organization's data. It is the HR team's duty to make sure that data is gathered, examined, and interpreted appropriately, adhering to national and international regulations. It should also determine and put into effect data access controls for every employee. The department is responsible for assisting in the handling of employee-related internet security events under the direction of the HR manager. In order to manage such occurrences and lessen the impact of the attack, it can be very helpful to develop a crisis management plan in conjunction with other departments.¹⁵

The utilisation of computer technologies and strategies for preventing online attacks on the business are particularly significant aspects of human resources education.¹⁶ Although there are many factors to take into account when creating a successful cyber security policy, legal actions are crucial in stopping and thwarting cybercrime. Every aspect, including criminalisation, jurisdiction, procedural powers, international collaboration, and internet service provider duty, requires legislation. In particular, criminalization, the creation of specific criminal offences for common cybercrime acts, is the main focus of national

¹³ Mimecast (2025): *Human Risk Management, Mitigating insider threats through proactive Human Risk Management in cybersecurity*, <https://www.mimecast.com/content/human-risk-management-in-cyber-security/>.

¹⁴ Foxall, D. (2025): *Six basic HR data security threats in 2025*, <https://www.hrmsworld.com/hr-data-security-threats.html>.

¹⁵ Talkspirit (2024): *Best Practices for Ensuring HR Data Security*, <https://www.talkspirit.com/blog/best-practices-ensuring-hr-data-security>.

¹⁶ Baltezarevic, B., Milutinovic, O., Baltezarevic, R., & Baltezarevic, V. (2020). Digital storage and online mediated memory. *International Review*, (1-2), 39.

cybercrime laws. Nonetheless, nations are realising more and more that other areas require legislation.¹⁷

According to a recent IBM analysis, data breaches cost businesses over \$4.5 million a year. According to the survey, American businesses spend twice as much. This budget is used to purchase specialised security technologies and hire cyber security experts. Social engineering and third-party exposure rank among the current top cyberthreats, according to security studies. Because it contains so much employee data, the HR department is vulnerable to these risks. For this reason, HR managers must implement internet security rules that safeguard the entire organisation in addition to enhancing the security of HR data. Astra recently reported that around 2,200 cyberattacks occur per day. Additionally, Gartner estimates that around 30% of cyberattacks will use AI to increase attack efficacy. These studies demonstrate the importance of HR data security and the necessity of putting in place a successful HR strategy.¹⁸

In addition to human error, which is said to be the weakest link in data security (as shown in Verizon's 2024 Data Breach Investigations Report, human error accounts for 68% of data breaches), which is primarily brought on by sharing credentials, using weak passwords, or falling for phishing schemes. The following are additional serious risks to the security of HR data: a). Insider attacks (An inexperienced person may unintentionally jeopardise data security, whereas a disgruntled employee with access to sensitive data may steal or leak it. Approximately 60% of all data breaches are caused by insider threats, according to ISACA. b) One of the most rapidly expanding cyberthreats is still ransomware. Cybercriminals are attacking HR systems in an attempt to obtain private employee information and demand money to restore it. In addition to inciting more attacks, paying these ransoms might be against new laws intended to limit ransomware payments. According to the IBM Cost of a Data Breach Report, the average cost of a ransomware attack on a company worldwide increased to \$4.5 million in 2023. c) Risks associated with remote and hybrid work: Workers who work from home frequently use personal devices or unprotected Wi-Fi networks, which leaves important HR data vulnerable to cyberattacks. 74% of companies have had cyber issues connected to remote work technologies, according to a Tenable study.¹⁹

Like health and safety training, information security awareness training has long been viewed as a box to be checked off a list. Regardless of whether they actually understand or interact with the content, they view it as just another task to

¹⁷ Sandage, J. et al. eds. (2013): "Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime*.

¹⁸ Talkspirit (2024): *Best Practices for Ensuring HR Data Security*, <https://www.talkspirit.com/blog/best-practices-ensuring-hr-data-security>.

¹⁹ Foxall, D. (2025): *Six basic HR data security threats in 2025*, <https://www.hrmsworld.com/hr-data-security-threats.html>.

finish. Many people are too busy, have strict deadlines to meet, or are just not interested in a training course that seems unrelated to their day-to-day jobs. Knowledge of information security can be interesting and essential to a company's risk management plan. We must go beyond conventional training techniques in order to do this.²⁰ Organisations should try to put in place a framework and plan that makes use of a variety of learning resources, such as interactive simulations and newsletters. Organisations ought to adopt the idea of human risk management, which has gained popularity in recent years.²¹

Strong cybersecurity is essential for businesses in the modern digital world to safeguard confidential information, reduce risks, and preserve operational integrity. It is crucial to put in place a tiered security framework. This strategy addresses weaknesses in an organization's infrastructure at various levels by combining several defensive techniques. Robust access controls significantly lower the danger of unauthorised data disclosure by limiting permissions based on job duties, especially through role-based access control (RBAC). Adherence to pertinent regulatory standards guarantees that security measures fulfil industry-specific and legal requirements, preventing fines and boosting credibility.²²

3. CONCLUSION

This paper underscores the key role of Human Resource Management (HRM) in cultivating a strong corporate security culture, drawing attention to the connections between human behavior, organizational values, and information security practices. By weaving together recruitment strategies, enhancing employee engagement, offering focused training, and assessing performance, HRM can have a significant impact on how employees understand and respond to security policies. The concept of Human Risk Management comes into play as a complementary framework designed to tackle specific behavioral vulnerabilities. This includes being susceptible to phishing, insider threats, and accidental data breaches, issues that can be more pronounced in remote and hybrid work situations.

The research indicates that relying solely on technical solutions won't cut it when it comes to keeping organizations secure. What's really needed is a human-centered approach to HR that's strategically aligned, which can help build resilience and

²⁰ Baltezarević, B., Baltezarević, R., & Baltezarević, V. (2018). Aktivnosti starijih osoba na onlajn društvenim mrežama. *Megatrend revija*, 15(3), 162.

²¹ Digitalxraid (2025): *The Future of Security Awareness: Integrating Human Risk and Security Awareness*, <https://www.digitalxraid.com/human-risk-management-security-awareness/>.

²² Law, B. (2025): *What are some examples of successful corporate security measures?*, <https://www.fixinc.io/blog/p/successful-corporate-security-measures>.

minimize human errors, one of the top culprits behind security breaches. According to the paper, it's crucial for us to move beyond the outdated checklist-style training. We should adopt more interactive and engaging learning experiences that continuously incorporate security awareness into our daily work culture.

There's been a noticeable uptick in interest in this field, but the existing literature still falls short when it comes to solid empirical research linking specific HRM practices to tangible security outcomes across various industries and cultural settings. Moving ahead, it's important for studies to focus on measuring the effectiveness of HR-driven security strategies, developing standardized metrics for evaluating security culture, and exploring how legal, technological, and organizational factors can either aid or obstruct the success of these initiatives.

By enhancing our grasp of the human aspect in cybersecurity through the perspective of HRM, organizations can foster more proactive, inclusive, and adaptable security cultures that are better prepared to tackle emerging threats.

Literature

- Al-Mekhlafi, A.-B. A. (2025): "Importance of Effective Human Resources Management in Creating a More Secure Work Environment by Improving Safety Culture", *International Journal of Intellectual Human Resource Management (IJIHRM)*, 5(01), 14-23.
- Al-Thunaihat, M. Y., Al-shawabkeh, A. A. & Al-baqor, K. K. (2020): "The Role of Human Resource Management Processes in Achieving Information Security: An Applied Study on Saudi Government Universities", *Management & Economics Research Journal*, 2(3), 1-23. DOI: 10.48100/merj.v2i3.107
- Baltezarevic, I. & Baltezarević, R. (2020): „Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku“, *Megatrend Revija*, 17(4), 27-40. DOI: 10.5937/MegRev2004027B
- Baltezarević, B., Baltezarević, R., & Baltezarević, V. (2018). Aktivnosti starijih osoba na onlajn društvenim mrežama. *Megatrend revija*, 15(3), 157-172.
- Baltezarevic, B., Milutinovic, O., Baltezarevic, R., & Baltezarevic, V. (2020). Digital storage and online mediated memory. *International Review*, (1-2), 34-41.
- Digitalxraid (2025): *The Future of Security Awareness: Integrating Human Risk and Security Awareness*, <https://www.digitalxraid.com/human-risk-management-security-awareness/>.
- Foxall, D. (2025): *Six basic HR data security threats in 2025*, <https://www.hrmsworld.com/hr-data-security-threats.html>.

- Karlsson, M., Karlsson, F., Åström, J. & Denk, T. (2022): "The effect of perceived organizational culture on employees' information security compliance", *Information and Computer Security*, 30(3), 382-401.
- Kumah, P. (2022): "The Role of Human Resource Management in Enhancing Organizational Information Systems Security", in: *Research Anthology on Business Aspects of Cybersecurity* (pp.300-325).
- Law, B. (2025): *What are some examples of successful corporate security measures?*, <https://www.fixinc.io/blog/p/successful-corporate-security-measures>.
- Milovanović, S., Lukinović, M. & Baltezarević, R. (2018): "Lični brend i integrisano marketing komuniciranje", *Megatrend revija*, 15(1), 177-186. DOI: 10.5937/MegRev1801177M
- Mimecast (2025): *Human Risk Management. Mitigating insider threats through proactive Human Risk Management in cybersecurity*, <https://www.mimecast.com/content/human-risk-management-in-cyber-security/>.
- Petrosyan, A. (2025): *Human risk management in global organizations 2024*, https://www.statista.com/statistics/1622615/human-risk-management-global/?srsltid=AfmBOooug_aRonZEfEQYjDazd0Q1vLnuU-5Kv6BllQZoyl73Ksc3u46y.
- Pujer, K. (2017): "Zarządzanie rozwojem pracowników. Założenia teoretyczne i praktyczne egzemplifikacje", In: Buzowska, B., Paliga, R., Pujer, K.: *Zarządzanie personelem w organizacji. Wybrane problemy teorii i praktyki*. Wydawnictwo Exante, Wrocław.
- Riemenschneider, C. K., Burney, L. L., & Bina, S. (2023): "The influence of organizational values on employee attitude and information security behavior: The mediating role of psychological capital", *Information and Computer Security*, 31(2), 172-198.
- Robinson, K. (2024): *HRM: The Difference Between Human Risk and Resource Management in Cyber Security*, <https://www.metacompliance.com/blog/cyber-security-awareness/hrm-human-risk-and-resource-management>.
- Sandage, J. et al. eds. (2013): "Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime*.
- Solomon, G., & Brown, I. (2021): "The influence of organisational culture and information security culture on employee compliance behaviour", *Journal of Enterprise Information Management*, 34(4), 1203-1228.
- Talkspirit (2024): *Best Practices for Ensuring HR Data Security*, <https://www.talkspirit.com/blog/best-practices-ensuring-hr-data-security>.

ULOGA UPRAVLJANJA LJUDSKIM RESURSIMA U UNAPREĐENJU KULTURE KORPORATIVNE BEZBEDNOSTI

Sažetak: Organizacije se sve više bore sa zadatkom zaštite svoje digitalne i fizičke imovine, posebno kako bezbednosne pretnje, kako iznutra tako i spolja, postaju sve složenije. Iako su tehnološka rešenja ključna, ljudsko ponašanje ostaje jedan od najznačajnijih i najranjivijih aspekata korporativnih bezbednosnih sistema. Ovaj rad ispituje ključnu ulogu upravljanja ljudskim resursima (HRM) u negovanju i jačanju čvrste korporativne bezbednosne kulture. Ispituje kako se različite HRM funkcije, uključujući regrutovanje, uvođenje u posao, obuku zaposlenih, sprovođenje politika i procenu učinka, mogu efikasno iskoristiti za oblikovanje ponašanja zaposlenih, smanjenje ljudskih grešaka i jačanje ukupne otpornosti organizacije. Ovaj rad predstavlja novo gledište na upravljanje ljudskim rizicima, koje nastoji da identifikuje, proceni i ublaži ranjivosti povezane sa ljudskim postupcima. Ovo uključuje probleme poput nasedanja na fišing prevare, insajderske pretnje i pogrešno rukovanje podacima. Posebno se bavi izazovima koji dolaze sa hibridnim i udaljenim radnim okruženjima, gde se bezbednosni rizici mogu povećati zbog širenja tehnologije i komunikacionih prepreka. Rad ističe koliko je važno uskladiti programe bezbednosne svesti sa ukupnom kulturom i vrednostima organizacije. Predlaže se udaljavanje od uobičajene obuke usmerene na usklađenost i umesto toga usvajanje angažovanijih pristupa usmerenih na ponašanje.

Ključne reči: upravljanje ljudskim resursima, Korporativna bezbednost, Ljudski rizici, Svest o sajber bezbednosti