Review scientific paper
UDK:37.036:316.75
DOI:10.7251/ZND2601657M

HUMAN RESOURCES AND CORPORATE SECURITY

***Danilo Mrković*[317]**
Associate Professor, Victoria International University, Mostar

Dragan Mišetić
***Associate Professor, University of Vitez*[318]**

Abstract: *Corporate security increasingly depends on how organizations manage their workforce, making the relationship between human resources and security a central concern of modern risk management. Employees influence security outcomes through their behavior, decision-making, access privileges, and adherence to procedures. Organizational culture further determines whether individuals treat security responsibilities as an integral part of their job or as secondary obligations. Legal requirements, including data protection and employment regulations, add another layer of complexity by requiring that monitoring, investigation, and access control measures protect both organizational assets and employee rights. At the same time, digital transformation has expanded the scope of HR responsibilities, as cloud-based platforms, remote work systems, biometric identification, and automated decision-making tools increase both efficiency and vulnerability. These developments position HR departments as key players in the enterprise security architecture, rather than as administrative support functions. Effective corporate security therefore depends on the integration of personnel management, governance structures, technological safeguards, and behavioral monitoring into a coordinated framework. Organizations that align HR strategy with security objectives are better able to anticipate risks, reduce internal vulnerabilities, and maintain operational resilience in an increasingly complex threat environment.*

Keywords: *corporate security, human resources management, security culture, organizational risk, digital HR systems.*

Introduction

Corporate security has traditionally been associated with physical protection, information security, and risk management systems. However, modern environments show that security risks increasingly stem from human behavior, organizational dynamics, and workforce practices. Employees can be a source of resilience, but also vulnerability, making human resources (HR) a central player in corporate security (Greitzer & Frincke, 2010). This shift reflects a broader understanding that technological defenses alone are not enough when organizational security depends largely on how people act, make decisions, and follow procedures. The relationship between HR and corporate security is based on the concept of human risk. Human risk refers to security threats that arise from employee actions, whether intentional or unintentional. These include insider attacks, negligence, policy violations, and data handling errors (Willison & Warkentin, 2013). While technical controls can limit exposure to risk, many incidents arise from behavioral factors such as lack of awareness, stress, dissatisfaction, or poor

[317] danilomrkovic@gmail.com
[318] misetic18@gmail.com

organizational structure. Research shows that insiders, employees, contractors, or partners with authorized access, can cause significant harm to organizations through data theft, sabotage, or fraud (Greitzer & Frincke, 2010). Such risks most often arise from individual dissatisfaction, sudden financial stress, workplace conflict, or disengagement. Human resources departments are often the first to notice changes in employee behavior, making them key in early risk identification. At the same time, HR departments must balance security concerns with legal, ethical, and privacy obligations, which complicates their role in monitoring and intervention. Human resources also shape corporate security through organizational culture. Organizational culture refers to shared values, beliefs, and norms regarding responsible workplace behavior. A strong culture encourages employees to follow policies and rules, report suspicious activity, and understand their role in the organization (Von Solms & Van Niekerk, 2013). The HR sector influences this culture through onboarding, training programs, communication strategies, and leadership development. Legal and regulatory pressures further link HR and security. Data protection laws, labor regulations, and industry standards impose requirements on how employee information is handled and how monitoring practices are implemented. For example, workplace surveillance used for security purposes must comply with privacy regulations and labor law restrictions (Voigt & Von dem Bussche, 2017). HR departments are responsible for implementing procedures that ensure employee compliance and trust. The legal dimension demonstrates that corporate security is not just a technical issue, but also a people management issue.

The rise of digital work environments further reinforces this relationship. Remote working, cloud-based HR systems, and digital identity management are expanding the exposure of sensitive employee and corporate data. HR platforms store personal data, making them valuable targets for attackers. At the same time, HR must often manage a remote workforce where direct supervision is limited, increasing reliance on trust, communication, and digital behavior guidelines.

In short, corporate security and human resources are increasingly interdependent. Employees represent both a key layer of defense and a significant risk factor. Human resources policies and practices shape the way individuals are selected, managed, trained, and monitored, which directly impacts the organization's security posture. Understanding these dynamics is critical to developing corporate security strategies that address not only technological threats, but also the human and organizational factors that determine resilience.

Security-Oriented Workforce Planning

Security-oriented talent management refers to the integration of security considerations into the recruitment, selection, placement, and workforce planning processes. In modern organizations, hiring decisions are no longer based solely on technical competence or experience. They also include assessments of reliability, integrity, and risk exposure, especially for positions that provide access to sensitive systems or confidential information. Research shows that personnel selection is one of the earliest and most effective stages in preventing internal security incidents because it determines who is granted access to the organization in the first place (Schultz, 2002).

Pre-employment screening is a fundamental element of corporate security. Screening procedures may include identity verification, credential validation, criminal background checks, and reference checks. These methods aim to reduce the likelihood of hiring individuals who pose a risk of fraud, espionage, or misconduct. Studies in organizational risk management show that background checks significantly reduce the likelihood of incidents in high-trust environments such as finance, government, and information technology sectors (Baer & Parkinson, 2007). Security-sensitive positions require more rigorous evaluation processes. Roles that involve privileged system access, financial authority, or intellectual property management often undergo enhanced screening procedures. These may include

behavioral interviews, psychological assessments, or integrity testing designed to identify traits associated with counterproductive work behaviors (Berry, Ones, & Sackett, 2007).

Workforce planning determines how many employees are needed, what skills they must possess, and how responsibilities are distributed. Poor workforce planning can create security gaps, such as overburdened staff with excessive system privileges or inadequate segregation of duties. Segregation of duties is a widely recognized control principle that prevents any one employee from having sufficient authority to commit and conceal misconduct (National Institute of Standards and Technology [NIST], 2020). Another important aspect is employee lifecycle management. Security risks often increase during transition phases such as onboarding, promotion, transfer, or termination. For example, newly hired employees may be unaware of security risks, while departing employees may still retain access credentials after leaving the organization. Studies of data breach incidents show that delayed deactivation of user accounts is a common cause of unauthorized system access (Verizon, 2023). Succession planning is also intertwined with corporate security. When key personnel leave unexpectedly, organizations may rush to appoint replacements without proper vetting or training. This creates temporary vulnerabilities that can be exploited by malicious actors or lead to operational errors. Structured succession planning reduces this risk by identifying and preparing qualified individuals in advance. Such preparation includes training, mentoring, and controlled escalation of privileges, which allows employees to take on responsibilities without compromising security controls (Rothwell, 2010). Training and continuous development represent another dimension of security-oriented human resource management. Security knowledge is not static; employees must adapt to new technologies, threats, and procedures. Human resources departments design these training initiatives, ensuring that competencies are maintained across the workforce and not concentrated in technical teams (Parsons et al., 2017).

Insider Threats, Human Risk, and Human Resource Countermeasures

Insider threats represent one of the most complex categories of organizational risk, as they originate from individuals who already have legitimate access to corporate systems and information. Unlike external attackers, insiders operate within the organization's trust boundaries, allowing them to bypass many technical safeguards. Research shows that insider incidents often cause greater financial and reputational damage than external attacks because insiders understand internal processes, security controls, and vulnerabilities (Cappelli, Moore, & Trzeciak, 2012). For this reason, corporate security strategies increasingly treat human behavior as the primary source of risk, rather than a secondary concern. Insider threats are classified into three categories: malicious, negligent, and compromised insiders. Malicious insiders intentionally cause harm for personal gain. Negligent insiders create risk unintentionally, often through carelessness or lack of awareness, such as mishandling data. Compromised insiders are legitimate users whose credentials or devices have been hijacked by external attackers. Studies show that careless behavior is responsible for a large proportion of security incidents, demonstrating that most insider risks stem not from malicious intent, but from human error (CERT Division, 2020).

Human resources departments play a key role in detecting early indicators of behavior associated with insider risk. Research shows that workplace stress, financial burden, interpersonal conflict, and job dissatisfaction can be associated with a higher likelihood of policy violations or malicious actions (Greitzer et al., 2014). HR professionals are often the first to notice such warning signs through complaints or attendance records. When properly trained, HR staff can identify patterns that may indicate elevated risk and coordinate with security teams to intervene before incidents occur. This preventive function is especially important because technical monitoring tools alone cannot reliably distinguish between legitimate and suspicious user activities without contextual human insight.

Effectively mitigating insider threats requires collaboration between HR, security, and management. Organizational studies show that cross-functional communication significantly improves threat detection and response because it combines behavioral information with technical evidence (Colwill, 2009). For example, a sudden change in system usage may appear suspicious from a technical perspective, but only HR can know that an employee is working extended hours on a legitimate project. Integrating these perspectives reduces false alarms and allows for more accurate risk assessments. HR policies also serve as formal countermeasures against insider threats. Clear codes of conduct and disciplinary procedures establish behavioral expectations and define consequences for violations. Such policies create a framework of accountability that discourages misconduct and strengthens trust in the organization. Research in deterrence theory shows that employees are less likely to engage in rule violations when policies are transparent, consistently enforced, and perceived as fair (Herath & Rao, 2009). Training programs are another important HR-led countermeasure. Empirical studies show that regular training significantly reduces employees' vulnerability to cyberattacks and increases compliance with organizational policies (Parsons et al., 2017). It is important to note that training must be continuous, not a one-time event. Human memory and attention decline over time, and threat tactics evolve. Continuous education ensures that employees remain capable of recognizing new risks**.**

Building and maintaining a safety culture through human resources

Corporate security does not depend solely on technologies or monitoring systems. It also depends on shared organizational attitudes and everyday behaviors. This collective dimension is commonly described as security culture, which refers to the set of values, norms, and practices that shape how employees perceive their responsibilities. Security culture determines whether rules are consistently followed, risks are reported in a timely manner, and whether employees view security as part of their role or as an external burden. Studies show that a weak security culture is strongly associated with policy violations, accidental data exposure, and vulnerability to attacks (Von Solms & Van Niekerk, 2013). Human resources departments play a central role in shaping and maintaining this culture because they manage the systems that influence employee behavior from entry to exit. Research on organizational culture shows that employee beliefs and habits are formed through processes such as job induction, performance evaluation, leadership, and internal communication (Schein, 2010). When security expectations are integrated into these processes, employees view them as standard workplace norms rather than exceptional requirements. Human resources therefore functions as an institutional mechanism through which security values are translated into everyday organizational practices. Onboarding is one of the most influential stages in establishing a security culture. During initial employment, individuals learn what behaviors are expected and what rules are taken seriously. If security training is included in orientation programs, employees develop an early awareness of risks such as password misuse or data handling errors. Empirical research shows that early training significantly improves long-term compliance because first impressions shape how employees interpret organizational priorities. Conversely, if security is introduced only later, employees may treat it as secondary to productivity or convenience (Parsons et al., 2017). Employees tend to prioritize tasks that affect evaluations, promotions, and compensation. When performance criteria include safety compliance, reporting responsibilities, or adherence to procedures, employees perceive safety as part of their professional responsibility. Behavioral studies show that aligning incentives with desired behavior increases compliance and reduces misconduct (Pahnila, Siponen, & Mahmood, 2007). Leader behavior further shapes cultural outcomes. Employees observe how managers treat safety procedures and imitate their behavior. If leaders bypass controls or ignore procedures, employees may interpret this as permission to do the same. Conversely, when leaders consistently follow policies and communicate the importance of safety, employees are more likely to adopt similar attitudes.

Organizational psychology research confirms that leadership is one of the strongest predictors of workplace norm formation (Schein, 2010). Ongoing communication is another essential factor. A safety culture cannot be maintained with one-time training alone. Threat environments change, technologies evolve, and employees forget information over time. Awareness campaigns, reminders, and scenario-based exercises help maintain attention and reinforce learning. Research shows that repeated exposure to security education reduces risky behavior compared to single training sessions (Jansson & von Solms, 2013). Resistance to security policies is a common organizational challenge. Employees may perceive policies as unnecessary, especially if they slow down daily tasks. Change management theory suggests that resistance is reduced when employees understand the purpose of policies and feel involved in the implementation processes (Kotter, 1996). Human resources departments can reduce resistance by explaining the reasons for security measures, gathering feedback from employees, and adjusting procedures to minimize unnecessary friction. Such involvement increases acceptance and improves compliance.

Legal compliance, HR policy and security management

The intersection between human resources and corporate security is strongly shaped by legal and regulatory obligations. Organizations must protect their assets and information while respecting the rights of their employees. This dual responsibility creates a complex governance environment in which HR departments play a central coordinating role. Security measures that affect employees, such as tracking or access control systems, must comply with labor law, data protection regulations, and industry standards. Failure to balance these requirements can expose organizations to legal penalties and damage their reputation. One of the most influential regulatory frameworks in this area is the European Union's General Data Protection Regulation (GDPR). The GDPR establishes strict rules for the processing of personal data, including employee information. It requires transparency, proportionality, and a legitimate purpose when collecting or monitoring personal data (Voigt & Von dem Bussche, 2017). For example, workplace surveillance used to detect insider threats must be justified and limited to what is necessary. Excessive monitoring can violate privacy rights and undermine employee trust. Labor law further restricts the way organizations can respond to suspected misconduct. Investigations involving employees must respect the principles of due process, confidentiality, and non-discrimination. Workplace compliance research highlights that properly structured internal policies reduce legal risk by ensuring consistent documented procedures (Kaptein, 2011). Therefore, HR ensures that security investigations follow clear protocols and are aligned with contractual obligations. Another important dimension relates to access control and role-based authorization. Legal compliance frameworks, such as ISO/IEC 27001, require organizations to define and document responsibilities for information assets. Annex A.6 and A.7 of ISO/IEC 27001 specifically address human resource security, including vetting, contractual clauses, and termination procedures (ISO, 2022). HR departments implement these controls by including confidentiality agreements in employment contracts and ensuring that access rights are updated when roles change. International operations introduce additional complexity. Multinational organizations must navigate different labor laws and data protection standards in different jurisdictions. What is legally acceptable in one country may be prohibited in another. Human resources departments coordinate local and global security policies to ensure compliance without fragmentation. This balancing act requires legal expertise and close collaboration with security leadership.

Digital HR technologies and new security risks

The digital transformation of human resource management has significantly improved efficiency, data availability, and strategic decision-making. At the same time, it has introduced new security risks that directly impact corporate security frameworks. Modern HR departments rely heavily on digital

systems such as Human Resource Information Systems (HRIS), cloud-based recruitment platforms, and employee analytics tools. These systems store large amounts of sensitive data, including personal identification data, payroll records, evaluations, and access data. Due to the concentration of confidential information, HR platforms have become attractive targets for cybercriminals. Studies on data breach patterns show that databases containing employee information are among the most valuable resources for attackers because they can be exploited for identity theft and financial fraud (Verizon, 2023). Cloud-based HR infrastructures are particularly important in this context. Many organizations have migrated HR systems to cloud environments to support remote work and centralized management. Cloud platforms enable HR teams to effectively manage a global workforce, but they also change the distribution of security responsibilities. Under the shared responsibility model, cloud service providers provide the infrastructure, while organizations remain responsible for user access control, identity management, and data governance (Mell & Grance, 2011). Security breaches often occur when organizations misunderstand this division of responsibility. For example, misconfigured access permissions can expose employee records to unauthorized users even when the cloud service provider's infrastructure remains secure. Therefore, HR departments must work closely with IT and security teams to ensure that cloud-based systems are properly configured and monitored.

Artificial intelligence has also become integrated into HR processes. AI tools are increasingly used for hiring screening, performance appraisals, and employee tracking. These technologies analyze large data sets to identify patterns in behavior or productivity. While such systems can improve decision-making efficiency, they introduce new categories of security and governance risks. Algorithmic systems rely on data integrity and system transparency. If compromised or manipulated, they can produce inaccurate assessments or reveal sensitive information. Research in information systems management shows that automated systems using AI can amplify risks when organizations fail to control access to data (Martin, 2019). Therefore, HR departments must ensure that AI tools meet standards for accuracy, accountability, and security.

Remote work technologies further complicate the relationship between human resources and corporate security. The expansion of distributed workforces has increased reliance on digital communication platforms and mobile devices. Each of these tools creates potential entry points for unauthorized access. Security guidelines emphasize that remote work environments require stronger authentication measures, encrypted connections, and strict device management policies (National Institute of Standards and Technology, 2020). Biometric identification systems are another emerging technology used in the integration of human resources and corporate security. Organizations are increasingly adopting fingerprint scanners, facial recognition systems, and voice authentication to control digital access. Biometric methods can improve security because they rely on unique physical characteristics rather than passwords, which can be guessed or stolen (Jain, Ross, & Nandakumar, 2011).

Conclusion

Security is no longer limited to technical safeguards or physical protection. It is shaped by human behavior, organizational structures, and institutional processes. Employees represent both a potential vulnerability and a critical line of defense. Because HR functions determine how individuals are selected, trained, evaluated, and managed, they directly impact the reliability of the organizational environment and the effectiveness of security systems. Analysis has shown that HR practices such as hiring vetting, role design, and lifecycle management influence who gains access to sensitive assets and how responsibly that access is used. Behavioral risks, including insider threats and negligent actions, show that many incidents stem from workplace dynamics rather than technological failure. HR therefore serves as an early detection point and warning signals that cannot be captured by automated monitoring alone. At the same time, organizational culture plays a decisive role. When

expectations, incentives, and leadership behaviors support responsible behavior, employees tend to internalize security norms and act accordingly. Legal obligations and governance structures further reinforce this interdependence. Compliance with data protection regulations, labor laws, and industry standards requires coordination between HR, security teams, and management. Policies governing monitoring, disciplinary action, and access rights must protect organizational assets while respecting individual rights. This balance cannot be achieved through technical controls alone. It requires procedural clarity, transparent communication, and institutional accountability. The increasing digitalization of HR systems adds another layer of complexity. Cloud platforms, automated decision-making tools, biometric systems, and remote work technologies increase efficiency, but also expand exposure to cyber risk and data misuse. As custodians of large amounts of sensitive information, HR departments now occupy a strategic position within the enterprise security architecture. Their decisions impact data protection, identity management, and access management across the organization. These factors demonstrate that corporate security is fundamentally interdisciplinary. Its effectiveness depends not only on technological capabilities, but also on people, organizational culture, and regulatory compliance. Strong collaboration between HR and security functions enables organizations to anticipate risks, respond systematically, and maintain trust among employees. In today's risk environments, sustainable security is achieved when HR and corporate security act as integrated components of a unified management framework.

Literature:

1. Baer, M. D., & Parkinson, D. (2007). Employee screening: Theory and practice. *Journal of Business and Psychology*, 22(2), 123–136.
2. Berry, C. M., Ones, D. S., & Sackett, P. R. (2007). Interpersonal deviance, organizational deviance, and their common correlates: A review and meta-analysis. *Journal of Applied Psychology*, 92(2), 410–424.
3. CERT Division. (2020). *Common sense guide to mitigating insider threats* (6th ed.). Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.
4. Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, 14(4), 186–196.
5. Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modelling for insider threat mitigation. In R. Probst, J. Hunker, D. Gollmann, & M. Bishop (Eds.), *Insider Threats in Cyber Security* (pp. 85–113). Springer, Boston, MA.
6. Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., & Hohimer, R. E. (2014). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. *Proceedings of the IEEE Security and Privacy Workshops*, San Jose, CA, 151–160.
7. Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems*, 47(2), 154–165.
8. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO Publishing, Geneva.
9. Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to biometrics*. Springer, New York.
10. Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6), 584–593.
11. Kaptein, M. (2011). Toward effective codes: Testing the relationship with unethical behavior. *Journal of Business Ethics*, 99(2), 233–251.
12. Kotter, J. P. (1996). *Leading change*. Harvard Business School Press, Boston, MA.
13. Martin, K. (2019). Ethical implications and accountability of algorithms. *Journal of Business Ethics*, 160(4), 835–850.

14. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800-145). National Institute of Standards and Technology, Gaithersburg, MD.
15. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Revision 5). U.S. Department of Commerce, Washington, DC.
16. Pahnila, S., Siponen, M., & Mahmood, M. A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences*, Waikoloa, Hawaii, 156–165.
17. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). The design of phishing studies: Challenges for researchers. *Computers & Security*, 68, 9–26.
18. Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate Publishing, Aldershot, UK.
19. Rothwell, W. J. (2010). *Effective succession planning* (4th ed.). AMACOM, New York.
20. Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass, San Francisco, CA.
21. Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6), 526–531.
22. Verizon. (2023). *Data breach investigations report*. Verizon Enterprise Security, New York.
23. Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer International Publishing, Cham.
24. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.
25. Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1–20.

LJUDSKI RESURSI I KORPORATIVNA SIGURNOST

Doc.dr Danilo Mrković
Victoria International University, Mostar

Prof.dr Dragan Mišetić
Sveučilište Vitez

Sažetak: *Korporativna sigurnost sve više ovisi o načinu na koji organizacije upravljaju svojom radnom snagom, što odnos između ljudskih resursa i sigurnosti čini središnjom brigom modernog upravljanja rizicima. Zaposlenici utječu na sigurnosne ishode svojim ponašanjem, donošenjem odluka, privilegijama pristupa i pridržavanjem postupaka. Organizacijska kultura dodatno određuje tretiraju li pojedinci sigurnosne odgovornosti kao sastavni dio svog posla ili kao sekundarne obveze. Pravni zahtjevi, uključujući propise o zaštiti podataka i zapošljavanju, dodaju još jedan sloj složenosti zahtijevajući da mjere praćenja, istrage i kontrole pristupa štite i organizacijsku imovinu i prava zaposlenika. Istodobno, digitalna transformacija proširila je opseg HR odgovornosti, jer platforme temeljene na oblaku, sustavi za rad na daljinu, biometrijska identifikacija i automatizirani alati za donošenje odluka povećavaju i učinkovitost i ranjivost. Ovi razvoji pozicioniraju HR odjele kao ključne igrače u sigurnosnoj arhitekturi poduzeća, a ne kao administrativne funkcije podrške. Učinkovita korporativna sigurnost stoga ovisi o integraciji upravljanja osobljem, struktura upravljanja, tehnoloških zaštitnih mjera i praćenja ponašanja u koordinirani okvir. Organizacije koje usklađuju HR strategiju sa sigurnosnim ciljevima bolje su sposobne predvidjeti rizike, smanjiti unutarnje ranjivosti i održati operativnu otpornost u sve složenijem okruženju prijetnji.*

Ključne riječi: *korporativna sigurnost, upravljanje ljudskim resursima, sigurnosna kultura, organizacijski rizik, digitalni HR sistemi.*