European Research Studies Journal
Volume XXIX, Issue 3, 2026

pp. 324-346

Personal Safety as an Element of an Organisation's Safety Management System

Submitted 23/07/26, 1st revision 18/08/26, 2nd revision 29/08/26, accepted 10/09/26

Marta Chodyka[1], Zbigniew Ciekanowski[2], Jarosław Wołejszo[3], Sławomir Mazur[4], Rafał Parczewski[5], Valeriy Kuznetsov[6], Piotr Lichograj[7]

Abstract:

Purpose: *The aim of this article is to identify and assess the significance of personal safety within an organisation's safety management system and to define the mechanisms enabling its systematic development. Particular attention has been paid to the dual role of the individual – as both a subject requiring protection and an active participant in processes influencing the organisation's safety level.*
Design/Methodology/Approach: *The main research question was formulated as follows: How does personal safety management influence the effectiveness of an organisation's safety management system? The hypothesis adopted was that systematic personal safety management–encompassing the identification and assessment of hazards, preventive measures, staff training, incident response, and continuous improvement–enhances the effectiveness of an organisation's safety system by mitigating human-factor risks and strengthening employees' ability to respond appropriately to hazards. The study employed a review and critique of the literature, an analysis of institutional documents and reports, a comparative analysis, and synthesis and inference. Selected standards and publications from ISO, NIST, ENISA and the International Labour Organisation were also analysed.*
Findings: *The analysis indicates that personal safety is an integral part of an organisation's security system and encompasses a much broader scope than the traditionally understood concept of employee protection. Interdependencies between physical, psychosocial, organisational, information and cyber threats were identified. The dual nature of the human factor was also demonstrated – an employee may constitute a potential source of vulnerability for the organisation, but, if properly trained, can simultaneously act as an*

[1]*John Paul II University in Biala Podlaska, Poland, ORCID: 0000-0002-8819-2451, e-mail: m.chodyka@dyd.akademiabialska.pl;*
[2]*The same as in 1, ORCID: 0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl;*
[3]*President Stanisław Wojciechowski University of Kalisz, Poland, ORCID: 0000-0002-7216-3496, e-mail: j.wolejszo@uniwersytetkaliski.edu.pl;*
[4]*Andrzej Frycz Modrzewski University in Kraków, Poland, ORCID: 0000-0002-5056-2280, e-mail: smazur@orange.pl;*
[5]*Military University of Technology, Poland, ORCID: 0000-0002-2603-0596, e-mail: rafal.parczewski1@wat.edu.pl;*
[6]*Railway Research Institute, Poland, ORCID: 0000-0003-4165-1056, e-mail: vkuznetsov@ikolej.pl;*
[7]*The same as in 1, ORCID: 0000-0002-1351-4874, e-mail: p.lichograj@dyd.akademiabialska.pl;*

active element of the security system. The results of the analysis confirmed the validity of the hypothesis.

Practical Implications: *The results can be utilised by organisations to design personnel security policies, conduct risk assessments, plan training, identify key posts, manage access rights, and prepare procedures for responding to incidents and crisis situations. The proposed approach may also serve as a basis for developing audit tools and indicators to assess an organisation's level of personnel security.*

Originality/Value: *The value of this study lies in integrating the employee protection perspective with the safety management perspective across the entire organisation, and in proposing a model framework for a personnel safety management system. The author's model comprises six interrelated stages: identification, assessment, prevention, preparation, response and improvement. The central element of the model is the individual, whilst its operation is supported by organisational, procedural, technical and educational measures. The result of implementing this approach should be a reduction in human-factor risks, increased staff protection, and strengthened business continuity and organisational resilience.*

Keywords: *Personnel safety, organisational safety, safety management, human factor, risk management, safety culture, organisational resilience, staff safety.*

JEL Codes: *J28, M54, M12, J81, K32.*

Paper type: *Research article.*

1. Introduction

Contemporary organisations operate in an environment characterised by rapid social, technological, economic and geopolitical change. The digitalisation of organisational processes, the development of new technologies, the widespread adoption of remote and hybrid working, the growing importance of information as a strategic resource, and the increasing scale of cyber threats necessitate the continuous adaptation of security management systems. In such circumstances, the human factor takes on particular significance.

This is because people remain not only an organisation's fundamental resource, but also individuals requiring protection, potential targets for threat actors, and participants in the processes responsible for maintaining the organisation's security and operational continuity.

The traditional approach to organisational security has largely focused on protecting physical assets, infrastructure, information, and technical systems. However, contemporary circumstances indicate that the effectiveness of security measures depends to a significant extent on the knowledge, competence, awareness and

behaviour of staff (Bogusz and Sidor, 2019, p. 177). Employees use IT systems, process information, make decisions, operate infrastructure and implement security procedures. At the same time, they may be exposed to physical, psychosocial, organisational, information-related and cyber threats.

Consequently, personal safety should be treated as an integral part of an organisation's safety management system, rather than solely as a matter of protecting employees from traditional workplace hazards. The importance of personal safety also stems from the individual's dual role within the safety system. On the one hand, the organisation is responsible for creating conditions that protect the lives, health, information and broadly understood safety of its employees.

On the other hand, an employee's actions can affect the safety of the entire organisation. Errors, inadequate knowledge, failure to follow procedures, poor information management, or vulnerability to social engineering attacks can lead to an incident. At the same time, a properly trained employee who is aware of the risks can act as an active component of the security system, identifying signs of a threat and taking appropriate action before serious consequences arise.

Expanding the list of risks affecting staff is becoming a particular challenge. In addition to traditional health and safety risks, modern organisations must take into account, amongst other things, work-related stress, work overload, violence and harassment, cyber threats, phishing, social engineering, credential theft, internal threats and the consequences of the uncontrolled use of new technologies. With advancing digitalisation, the boundary between human security and the security of an organisation's information and systems is becoming increasingly blurred. ENISA points out that phishing remains one of the most significant mechanisms for gaining initial access to systems, underscoring the importance of the human factor in countering modern cyber threats.

This necessitates the adoption of a systematic approach to personnel security, covering the entire cycle of an individual's tenure within an organisation – from recruitment and induction, through the performance of duties, training, skills development, and access management, to a change of role or the end of employment. Personnel security should, at the same time, be linked to risk management, information security, cybersecurity, health and safety at work, crisis management and business continuity. Such an approach allows people to be viewed not only as a potential source of vulnerability, but above all as one of the key assets that build an organisation's resilience.

2. The Nature and Significance of Personnel Security in the Functioning of an Organisation

Modern organisations operate in an environment characterised by rapid technological, social and economic change, as well as the growing interdependence

of organisational processes. This leads to a systematic expansion of the range of threats that may affect both the organisation's ability to achieve its objectives and the safety of its employees. The traditional approach to organisational security, focused primarily on the protection of infrastructure, physical assets and information, is therefore insufficient.

The human factor is becoming increasingly important, as employees' knowledge, behaviour, competencies, and decisions directly influence the organisation's ability to identify threats, mitigate risks, and respond to crises (Khadka and Ullah, 2025).

In this context, personal safety should be regarded as a fundamental component of an organisation's safety system. It should not be equated solely with protecting employees from accidents, violence or other direct physical threats. In a broader sense, it encompasses the creation of organisational, procedural, technical and social conditions that enable employees to carry out their assigned tasks safely and minimise the likelihood of incidents occurring that could have negative consequences for both the individual and the organisation as a whole.

Research on the human dimension of safety indicates that an individual's behaviour is shaped not only by their knowledge and competencies, but also by organisational culture, organisational structure, communication, social norms and the nature of the working environment (Larena-Luengo *et al.,* 2026).

Personal safety can be analysed from two interrelated perspectives. The first focuses on the safety of the individual operating within the organisation, whilst the second focuses on the individual's importance to the organisation's safety. This distinction is significant because an employee is both a person requiring protection and a participant in the safety system responsible for carrying out specific tasks and adhering to applicable procedures. Their actions may enhance the organisation's resilience, but inappropriate behaviour, errors, or a lack of relevant competencies may lead to new vulnerabilities (Metalidou *et al.,* 2014).

From a security management perspective, it is particularly important to move away from treating staff solely as a potential 'weak link'. Contemporary research indicates that a properly trained employee can constitute a significant security asset. Appropriate competencies, threat awareness, knowledge of procedures and the ability to recognise unusual situations can enhance an organisation's capacity to identify incidents at an early stage.

Therefore, management actions should aim to transform the human factor from a potential source of vulnerability into an active element of the organisation's security system (López-Muñoz *et al.,* 2025). This approach means that personnel security should be treated as an interdisciplinary field, situated at the intersection of security studies, management sciences, organisational psychology, human resource management and information security. In practice, this means that technical,

organisational and human risk determinants must be considered simultaneously. An approach that integrates these three perspectives allows for a more comprehensive assessment of an organisation's vulnerabilities than an analysis limited solely to technical safeguards (Yang, King, and Yang, 2008).

An organisation's security management system can be viewed as a set of interrelated elements designed to identify threats, analyse risks, plan security measures, respond to incidents and improve existing solutions. The human factor is present in each of these areas. It is employees who identify specific signs of threats, make decisions, use IT systems, have access to information and infrastructure, implement security procedures, and participate in emergency response. The effectiveness of a security system, therefore, depends not only on the technologies employed but also on people's competencies and behaviour (Imam, 2023).

Security awareness is of particular importance in this regard. Employees should not only be familiar with formal procedures but also understand their purpose and the consequences of noncompliance. The mere introduction of a security policy does not, in itself, guarantee appropriate behaviour by staff. Research indicates that gaps in employees' knowledge and skills can be exploited by threat actors even in organisations with advanced technical security measures (Ani, He, and Tiwari, 2019).

Staff security, therefore, requires consideration of the entire cycle of an employee's tenure within the organisation. This begins as early as the recruitment stage, when the organisation defines the required competencies, the scope of responsibilities, and the level of access to resources (Bogusz, 2021, p. 229). Subsequent elements include employee induction, communication of security policies, training, granting authorisations, periodic competence assessments, monitoring compliance with procedures, and proper management of job changes or the termination of employment (Bogusz, 2025, p. 60).

Understood in this way, personnel security is not a one-off activity, but a process requiring continuous management. It is also important to consider the relationship between people and technology. As organisational processes become digitised, employees gain access to an ever-increasing number of systems, data and communication tools. This increases the significance of their decisions and behaviour for the security of the entire organisation.

Research on cybersecurity indicates that human-related vulnerabilities may stem, among other things, from cognitive, psychological, behavioural, social, and organisational factors (Khadka and Ullah, 2025). Personal security should not be limited to a single type of threat. A proper analysis of it requires consideration of several interrelated dimensions. These include, first and foremost, the physical, psychological, social, informational, cyber and organisational dimensions.

These dimensions do not operate independently. An incident in one area may have consequences in other areas, leading to a cumulative risk effect.

The physical dimension primarily concerns protecting employees' lives and health and ensuring a safe working environment. It includes, amongst other things, protection against accidents, violence, infrastructure risks, disasters, fires and other situations that may cause direct harm to health.

The psychological and social dimension*,* on the other hand, encompasses organisational conditions that influence an employee's functioning, including interpersonal relationships, organisational culture, communication styles, workload and a sense of influence over the tasks being carried out. Recent research shows that organisational culture can play a central role in shaping the working environment, coordinating relationships and influencing how staff perceive risk (Larena-Luengo *et al.,* 2026).

The information and cyber dimensions take on particular significance in organisations that utilise digital technologies. Employees have access to information, personal data, ICT systems, and resources essential to business continuity. Human error can lead to the unintentional disclosure of information, data loss or unauthorised access. For this reason, raising security awareness is a fundamental mechanism for reducing vulnerabilities related to human factors (Metalidou *et al.,* 2014).

One of the most important factors determining the level of personnel security is the security culture. Management plays a significant role in shaping this culture; their attitudes, decisions and the way they communicate priorities influence employees' behaviour and their approach to applicable security rules. Leadership should therefore be regarded as one of the factors determining the development of an organisation's safety culture (Ciekanowski *et al.,* 2025).

This encompasses the values, norms, attitudes and behavioural patterns relating to how safety rules are perceived and respected. In an organisation characterised by a well-developed safety culture, employees do not treat procedures merely as a formal obligation, but understand their role in protecting other people and the organisation's assets. The importance of a safety culture also stems from the fact that not all employee behaviour can be regulated by detailed procedures.

In new or unforeseen situations, employees often have to assess the situation independently. In such cases, their previous experience, knowledge, awareness of risks and the norms operating within the organisation take on particular significance. Research into an organisation's preparedness to counter cyber threats, therefore, highlights the need to assess factors such as awareness, employee behaviour and safety culture (Georgiadou, Mouzakitis, and Askounis, 2022). In this regard, the security culture should be shaped by the organisation's management.

The attitudes of managers, the way priorities are communicated, and the actual enforcement of established rules all influence whether staff perceive security as a key organisational value. Of particular importance are the clear definition of responsibilities, the promotion of continuous learning, and the creation of an environment in which employees can report threats and irregularities.

Contemporary research into the human dimension of cybersecurity identifies the development of a security culture, a clear division of roles and continuous learning as key management activities that enhance an organisation's security (López-Muñoz *et al.,* 2025). The importance of personnel security becomes particularly evident in situations of disruption and crisis. An organisation may have extensive technical safeguards and procedures in place, but their effectiveness depends on the staff's ability to respond appropriately. Staff must be able to recognise a threat, communicate the information, take appropriate action and continue to carry out key processes under conditions of heightened risk.

From this perspective, personnel safety becomes an element of organisational resilience. Properly trained staff are not merely the objects of protection, but a resource enabling the organisation to adapt to changing conditions. An interdisciplinary approach to the human factor highlights the need to analyse safety through the interrelationships between people, technology and the organisation, rather than considering these elements in isolation (Pollini *et al.,* 2022).

It can therefore be assumed that personal safety fulfils a dual function within an organisation. On the one hand, its aim is to protect employees from hazards arising from the working environment and the organisation's surroundings. On the other hand, a properly trained, aware and competent employee becomes one of the organisation's fundamental protective mechanisms. This interdependence justifies the inclusion of personal safety within a systematic safety management framework, alongside physical, information, cyber, infrastructure and business continuity safety.

Consequently, personnel safety should be understood as a continuous and deliberately managed process of ensuring an appropriate level of protection for employees, whilst simultaneously developing their competence, awareness, responsibility and behaviours that serve the safety of the entire organisation. This approach allows us to move away from viewing the employee merely as a potential source of risk. The individual becomes an active participant in the security system, whose preparedness and attitude can enhance the organisation's ability to prevent threats, respond to incidents and maintain business continuity.

3. Personal Safety Threats in the Modern Organisation

Personal safety in a modern organisation is determined by a complex array of threats occurring both within the organisation and in its wider environment. Technological changes, the digitalisation of work processes, growing dependence on ICT systems,

new models of performing professional duties, and changing social relationships mean that employees are exposed not only to traditional physical threats but also to psychosocial, information-related, and cyber threats. At the same time, staff themselves may – consciously or unconsciously – become a source of risk to the organisation. This necessitates a shift away from a one-sided understanding of personal safety as the protection of the individual towards an approach that accounts for the interdependence between employee and organisational safety.

The primary category comprises risks to individuals' physical safety. These may arise from the nature of the work performed, the condition of the infrastructure, the machinery and equipment used, contact with hazardous substances, transport, the movement of staff, or the occurrence of extraordinary events. Physical risks should not, however, be analysed in isolation from organisational conditions. Poor workplace organisation, excessive workloads, time pressure, understaffing or failure to follow procedures can increase the likelihood of errors and accidents.

The International Labour Organisation points out that the working environment can give rise to chemical, ergonomic, physical, biological and psychosocial hazards, which call for a comprehensive approach to worker protection (ILO, 2022). Risks associated with violence and inappropriate interpersonal behaviour are also a significant aspect of personal safety. These may take the form of physical aggression, threats, intimidation, bullying, harassment, discrimination, psychological violence or other behaviours that violate a worker’s integrity. This is not a marginal issue.

According to data cited by the International Labour Organisation, more than one in five people in employment have experienced violence or harassment in connection with their work. Importantly, these risks are not limited to the workplace in the traditional sense, but may also occur during business travel, work-related events, commuting, digital communication and when working from home (Karimova and Boehmer, 2024).

Psychosocial risks are of particular significance. High demands placed on employees, pressure to achieve results, unclear responsibilities, inadequate support from line managers, interpersonal conflicts, or poor work organisation can cause long-term psychological strain. From the perspective of an organisation’s safety system, this issue should be considered more broadly than merely as a matter of employee well-being. A deterioration in mental and physical health can, in fact, affect concentration, decision-making, the ability to identify hazards and compliance with procedures.

The ILO highlights the link between poor work organisation, high levels of stress and the risk of violence and harassment, whilst also pointing to the need to incorporate psychosocial risks into occupational health and safety management systems (ILO, 2024).

Another significant issue is that some workplace risks remain difficult for an organisation's management to identify. This applies in particular to psychological violence, discrimination, workplace bullying and long-standing conflicts. Employees may fail to report incidents due to fear of consequences, a lack of trust in their superiors, a lack of knowledge of available procedures, or the belief that reporting will not lead to a resolution. A global study by the ILO, the Lloyd's Register Foundation and Gallup highlights the significance of barriers to reporting cases of workplace violence and harassment (ILO, Lloyd's Register Foundation and Gallup, 2022).

With the ongoing digitalisation, information and cyber threats are becoming an increasingly significant category of risks to personal security (Skóra and Bogusz, 2025, p. 312). Organisations' growing reliance on information and communication technologies means that cybersecurity is becoming a fundamental area of modern security management. Effectively countering these threats requires combining technical safeguards with organisational measures and developing staff knowledge and awareness (Ciekanowski *et al.,* 2024).

Employees now operate in an environment where even the performance of basic duties requires the use of email, IT systems, mobile devices, cloud services, communication platforms and databases. On the one hand, these solutions increase organisational efficiency; on the other, they expand the attack surface. People have become a primary target of social engineering attacks, which exploit specific behaviours, errors, or human vulnerabilities to gain access to information or services (ENISA, 2025). Phishing is of particular significance, as it remains one of the primary methods of gaining access to an organisation's resources.

According to the ENISA Threat Landscape 2025, phishing accounted for 60 per cent of the analysed points of initial access to systems, whilst the exploitation of technical vulnerabilities accounted for 21.3 per cent. ENISA also highlights the growing use of artificial intelligence to enhance the effectiveness of phishing and automate social engineering activities. This means that the development of AI not only supports organisations in terms of security but also increases the capabilities of actors who carry out activities that directly target employees (ENISA, 2025).

From a personal security perspective, the evolution of social engineering methods is particularly dangerous. An attack no longer needs to be limited to an email containing a malicious attachment or link. Increasingly, SMS messages, instant messaging apps, telephone calls, and techniques that enable more convincing impersonation of line managers, colleagues, or representatives of organisations are being used.

The Verizon Data Breach Investigations Report 2026 indicates that the effectiveness of mobile social engineering attacks utilising, amongst other things, fake text messages and telephone calls was 40 per cent higher than that of traditional email

phishing (Verizon, 2026). Cyber threats also highlight the employee's dual role mentioned earlier. On the one hand, the individual is the target of the attack, as the attacker attempts to exploit their trust, lack of knowledge, inattention or time pressure.

On the other hand, an employee's decision can directly affect the security of the entire organisation. Opening an infected attachment, handing over credentials, using the same password across multiple services, sending information to the wrong recipient, or using an unauthorised application can lead to an incident affecting a much wider range of resources than a single workstation. Verizon's data indicate that the use of compromised credentials was the initial access vector in 22 per cent of the breaches analysed in the DBIR 2025, highlighting the importance of proper identity management and user behaviour (Verizon, 2025).

This problem is further complicated by the widespread adoption of generative artificial intelligence. Employees may use publicly available AI tools without the organisation's knowledge, inputting work-related information, customer data, excerpts from documentation or other content into them; processing such data outside a controlled environment may lead to a breach of security policies.

According to the DBIR 2026, the use of unauthorised tools by employees, referred to as 'shadow AI', has risen to 45 per cent, indicating the emergence of a new area of risk at the intersection of human behaviour, information management and technology (Verizon, 2026).

Internal threats, often referred to as *'insider threats'*, also remain a key element of personnel security analysis. Not every incident caused by an employee is deliberate. Insider threats can be considered in relation to both deliberate actions intended to harm the organisation and unintentional behaviour resulting from errors, ignorance, insufficient training or failure to follow procedures.

From a security management perspective, this distinction is very important. Countering deliberate actions requires, amongst other things, appropriate access control and monitoring, whilst minimising unintentional errors requires, above all, adequate staff training, the design of clear procedures and the fostering of security awareness.

At the same time, one cannot assume that every hazard arising from human behaviour is solely the consequence of an employee's inappropriate attitude. Errors may result from poorly designed processes, excessive workload, time pressure, a lack of clear procedures, insufficient training, or the use of systems that do not account for user limitations.

Consequently, responsibility for personal safety should be shared between the employee and the organisation. The role of a safety management system is to create

conditions that minimise the likelihood of errors occurring and, should they occur, to limit their potential consequences. Another category comprises risks associated with access to information and authorisations. Modern employees may have access to personal data, financial records, customer data, trade secrets, production systems or an organisation's critical infrastructure. Excessive access rights increase the potential consequences of both errors and deliberate actions.

Therefore, personnel security should encompass not only the protection of the employee but also the management of their access to resources in accordance with the scope of their duties. It is particularly important to update access rights when an employee changes roles and to effectively revoke them upon termination of employment.

External factors also influence the level of personnel-related threats. Organisations and their staff may be exposed to the effects of armed conflicts, geopolitical tensions, economic crises, natural disasters, epidemics, infrastructure disruptions, criminal activities or disinformation campaigns. ENISA points out that geopolitics remains a significant factor shaping the activities of actors conducting cyber operations, and actions targeting organisations may include both traditional cyber-attacks and the manipulation and interference with information (ENISA, 2024; ENISA, 2025).

These threats may have a particularly severe impact on staff at public organisations and entities operating in sectors critical to national security. In the ENISA Threat Landscape 2025, public administration accounted for 38.2% of the incidents analysed in the European Union, transport for 7.5%, digital infrastructure and services for 4.8%, finance for 4.5%, and the manufacturing sector for 2.9%. More than half of the incidents analysed – 53.7% – concerned critical entities as defined by the NIS2 Directive (ENISA, 2025).

Cyber threats targeting public administration are, moreover, perceived as one of the key challenges to the security of European Union member states, which further highlights the importance of protecting staff in critical organisations (Grudniewski *et al.,* 2026). These figures indicate that staff security should also be analysed in the context of the organisation's importance to the wider security system.

Furthermore, modern personnel-related risks are characterised by the potential to reinforce one another. An employee working under time pressure, suffering from fatigue or caught up in an organisational conflict may be more prone to making mistakes. Such a mistake, in turn, may be exploited in a cyberattack, resulting in data loss, process disruption, and additional pressure on the staff responsible for dealing with the aftermath of the incident.

This means that physical, psychosocial, organisational, information and cyber threats should not be analysed in complete isolation. They form a system of

interdependencies in which the occurrence of one factor may increase the organisation's vulnerability in other areas. From the perspective of a safety management system, it is therefore of paramount importance to identify the sources of risk and assess their impact on both employees and the organisation.

Personal safety should cover the entire cycle of the employee's relationship with the organisation – from recruitment and induction, through the performance of duties, changes in scope of responsibility and access rights, right up to the end of the employment relationship. It is particularly important to recognise the interdependence between an employee's mental and physical state, organisational culture, level of risk awareness, the technologies used, and the quality of safety procedures.

An analysis of contemporary threats, therefore, leads to the conclusion that an individual is simultaneously the subject of protection, a potential target for an attacker, and an active element of the organisation's security system. It would therefore be unjustified to reduce personnel security solely to the protection of employees or, conversely, to treat staff primarily as a source of risk.

The correct approach should integrate both perspectives. An organisation should protect individuals from threats whilst also developing their knowledge, skills and awareness to enable them to play an active part in ensuring security. This approach forms the starting point for building a comprehensive personnel security management system.

4. Personnel Safety Management as Part of an Organisation's Safety System

Effectively ensuring personnel safety requires a shift away from ad hoc measures towards a systemic approach, in which the protection of personnel is permanently integrated into the organisation's management processes. A systemic approach takes on particular significance in view of the growing complexity of an organisation's security environment. This is because security management requires integrating human resources, organisational solutions, procedures, and technical instruments into a coherent system that enables risks to be identified and mitigated (Chrzaszcz *et al.,* 2024).

Personal safety should not be treated solely as the domain of health and safety services, human resources departments or units responsible for information security. The contemporary security environment is characterised by the interplay of physical, psychosocial, organisational, information and cyber threats. The response to this complexity should be a management system that integrates threat identification, risk assessment, preventive measures, staff preparedness, incident response and the continuous improvement of established solutions. Such an approach is consistent with the logic of modern management systems, in which significant importance is

attached to leadership, risk assessment, employee participation, monitoring of results and continuous improvement (ISO, 2018).

The starting point for personnel security management should be the identification of human resources and the threats to which individual groups of staff are exposed. This is because not every member of staff within an organisation is subject to the same level of risk. Different types of risks apply to employees carrying out manual labour, management staff, personnel with access to sensitive information, ICT system administrators, employees in direct contact with customers, and those performing duties outside the organisation's premises.

This means there is a need to create risk profiles that take into account the role, scope of responsibility, working environment, authorisations held, access to resources and the potential consequences of misconduct. ISO 45001 bases occupational health and safety management on, amongst other things, hazard identification, risk assessment, action planning and system improvement, which may also serve as an important point of reference for a broader approach to personal safety (ISO, 2018).

A personal risk assessment should take into account not only the likelihood of a specific event occurring, but also its possible consequences for individuals and the organisation. In practice, this means analysing, amongst other things, the risks of loss of health or life, incapacity for work, disclosure of information, loss of a key employee's expertise, operational errors, disruption to business continuity, or the exploitation of staff in social engineering activities.

Of particular importance here is the identification of critical roles and functions whose temporary unavailability could significantly limit the organisation's ability to carry out its core tasks. This approach means that personnel security management is linked not only to the protection of employees, but also to risk management and organisational resilience.

A key element of the system is an appropriate personnel security policy that sets out objectives, areas of responsibility, staff requirements, and guidelines for conduct in situations that may pose a threat. Such a document should be integrated with other policies in force within the organisation, particularly those relating to information security, health and safety at work, personal data protection, business continuity, crisis management and cybersecurity.

Integration is of particular importance because personal safety cannot be effectively ensured by systems operating independently of one another and without information exchange. ISO/IEC 27001 specifically emphasises the systematic establishment, implementation, maintenance and continuous improvement of information security management, covering assets such as financial information, intellectual property, employee data and information entrusted by third parties (ISO, 2022).

Personnel security management should begin as early as the recruitment stage. The selection of staff should be considered not only in terms of professional qualifications, but also in terms of the security requirements associated with a specific post (Bogusz, 2024, p. 120). This is of particular importance in the case of roles involving access to sensitive information, IT systems, technical infrastructure, financial resources or other assets of significant importance to the organisation.

The scope of verification procedures should, of course, be proportionate to the nature of the post and comply with applicable law. The primary aim is not to foster a culture of mistrust towards employees, but to minimise situations in which a person lacking the appropriate qualifications or training is entrusted with tasks that pose an above-average risk. The next stage is the proper induction of the employee. The initial period of employment should involve not only familiarising the employee with their duties, but also explaining how the safety system operates.

The employee should be aware of the hazards associated with their role, what information they are permitted to use, what authorisations they hold, what actions are prohibited, and to whom and how they should report incidents. A lack of adequate initial preparation may lead to a situation where an employee is formally familiar with the regulations but does not understand their actual responsibility for safety. The training system is of particular importance. It should not rely solely on providing an employee with a large amount of information on a one-off basis.

The nature of modern threats requires regular updating of knowledge and the development of practical response skills. The NIST Cybersecurity Framework 2.0 identifies awareness and training as a separate category of protective function, highlighting the need to provide staff with the appropriate knowledge and competencies to carry out their tasks whilst taking cyber risks into account (Pascoe *et al.,* 2024).

Training on personal security should, at the same time, be tailored to the actual threats present within the organisation. A different scope will be required for management staff, another for administrative staff, and yet another for ICT infrastructure administrators. In the field of cybersecurity, ENISA highlights the importance of properly designed awareness-raising activities and of taking into account the behavioural and psychological aspects of human behaviour in the digital environment (ENISA, 2021; 2024).

This implies the need to move away from a model in which training is treated as a mere formality that serves only to confirm compliance with organisational requirements. Effectiveness should be assessed through changes in staff behaviour. In practice, situational exercises, phishing simulations, incident response workshops, knowledge tests, evacuation scenarios and crisis simulations can be used. ENISA points out that the use of gamification elements and practical experiences can also facilitate the understanding of cybersecurity issues and increase staff engagement in

awareness-raising activities (ENISA, 2024). An extremely important element of personnel security management is the management of access to the organisation's resources. An employee should have only the access rights necessary to carry out the tasks entrusted to them.

Excessive access amplifies the consequences of a potential error or deliberate action. For this reason, the scope of authorisations should be regularly reviewed, particularly in the event of a change in position, remit or organisational structure. A particularly critical moment is the termination of employment, when access to systems, premises, documentation and other protected resources should be effectively revoked. More broadly, this approach is consistent with the logic of information risk management, as supported by the requirements of the ISO/IEC 27000 series (ISO, 2022).

At the same time, personnel security management should not result in an excessive focus on employee monitoring. Building a system based solely on monitoring, restrictions and sanctions may lead to a decline in trust, the concealment of errors and a reduced willingness to report irregularities. It is far more important to create an environment in which staff understand their responsibilities and can report risks without fear of unjustified consequences. ISO 45001 particularly emphasises the importance of consultation and employee participation in the operation of the occupational health and safety management system (ISO, 2018).

Management plays a key role in this regard. If management fails to follow established procedures, tolerates circumvention of safety measures, or signals that achieving results is more important than safety, employees may adopt a similar approach. The commitment of top management is therefore a prerequisite for an effective management system. ISO 45001 explicitly highlights the importance of leadership and management commitment, as well as worker participation, as elements of the OH&S system (ISO, 2018).

However, the role of management should be understood more broadly than simply approving safety documentation. Managers should be involved in setting priorities, ensuring adequate resources are provided, responding to reported incidents, and assessing whether existing safety mechanisms remain appropriate to the changing risk environment. It is particularly important to establish a clear division of responsibilities. Failure to identify those responsible for specific processes may lead to a situation in which security is formally everyone's responsibility, yet in practice no one is accountable for it.

The modern approach to security management also highlights the need to treat risk as a management issue, rather than a purely technical one. The NIST Cybersecurity Framework 2.0 has expanded the previous structure to include the **'Govern'** function, which covers, among other things, risk management strategy, expectations, policies, roles, accountability, and oversight. This function complements the

'Identify', 'Protect', 'Detect', 'Respond' and 'Recover' areas and emphasises that responsibility for security should be linked to the management of the entire organisation (Pascoe *et al.,* 2024).

From a personal safety perspective, the ability of staff to report incidents and potentially dangerous situations is also of particular importance. The organisation should have simple and unambiguous reporting channels in place to enable the reporting of security breaches, suspected phishing attempts, unauthorised access, accidents, violence, bullying, or other irregularities. Information of this kind should then be analysed not only to resolve individual cases, but also to identify systemic causes. The response to an incident should be linked to the organisation's learning process.

Simply restoring normal operations after an incident is insufficient unless its causes are identified and measures are put in place to prevent a similar situation from recurring. The analysis should therefore include determining whether the problem stemmed from human error, an inappropriate procedure, a lack of training, a faulty technical solution, an excessive workload on an employee, or a combination of several factors. NIST CSF 2.0 covers the entire risk management cycle through the functions of Govern, Identify, Protect, Detect, Respond and Recover, which emphasises the need to combine prevention with response and the restoration of the organisation's capabilities following an incident (Pascoe *et al.,* 2024).

A personal safety management system should also take into account the protection of staff during emergencies. The organisation must define procedures for dealing with, amongst other things, fires, infrastructure failures, power cuts, cyber-attacks, natural disasters or other events that limit the ability to carry out tasks. Appropriate procedures should not only specify how to secure infrastructure and information, but, above all, set out the principles for protecting life and health, communicating with staff, evacuating, organising replacements, and maintaining the operation of critical processes. ISO 45001 recognises emergency preparedness and response as one of the key elements of a systematic approach to occupational safety (ISO, 2018).

Ensuring staff replaceability is also of great importance. An organisation's excessive reliance on individual persons can lead to significant operational risk. Illness, an accident, resignation or the temporary unavailability of a person possessing unique knowledge may cause an important process to be interrupted.

Therefore, personnel security should include identifying key roles, establishing stand-ins, documenting knowledge and developing the competencies of more than one person in critical areas. In this respect, personnel security becomes directly linked to business continuity and organisational resilience.

It is equally important to continuously monitor the effectiveness of the system. The organisation should define indicators to assess the actual level of personnel security.

These may include the number of incidents, accidents and near-misses, the number of reported irregularities, the results of safety drills and tests, the level of participation in training, the frequency of procedural breaches, audit findings, incident response times and staff awareness levels (Bogusz, 2018, pp. 13-14). The assessment should not be limited to simply counting incidents. A low number of reports may, in fact, indicate either a high level of safety or a poor reporting culture.

The personnel security audit remains an important tool. It should encompass not only a review of documentation but also an assessment of the practical application of the adopted measures. The audit may analyse the method of granting authorisations, the up-to-date nature of training, staff preparedness to respond, the effectiveness of reporting channels, the implementation of procedures concerning individuals leaving the organisation, and the alignment of actual practices with the declared security policy. Audits and management reviews form part of the continuous improvement approach inherent in both the ISO 45001 and ISO/IEC 27001 standards (ISO, 2018; ISO, 2022).

A key element of the system should be the fostering of a security culture. ENISA points out that cybersecurity culture programmes should incorporate knowledge from organisational sciences, psychology, law, and cybersecurity, thereby confirming the interdisciplinary nature of the human dimension of security (ENISA, 2018). However, a security culture does not arise simply from drafting a policy or conducting training. It is the result of a long-term process during which specific values and behaviours become part of the organisation's day-to-day operations.

Consequently, it can be proposed that an organisation's personnel security management system should be based on six interrelated stages:

- identification;
- assessment;
- prevention;
- preparation;
- response;
- improvement.

The effectiveness of safety management systems depends on an organisation's ability to systematically identify hazards, assess risks, implement appropriate protective measures and adapt them to changing operating conditions. Of particular importance here is the integration of organisational, technical and personnel solutions, as well as the continuous improvement of the adopted safety mechanisms (Chodyka *et al.,* 2026)." The individual elements form a cycle, the essence of which is the continuous adaptation of the solutions employed to changes occurring both within the organisation and in its environment. The structure of the proposed model is shown in the figure below (Figure 1).

Figure 1. *Model of an organisation's personnel safety management system.*

Source: Own work.

During the identification phase, the organisation identifies its human resources, key roles and threats. The assessment phase determines the level of risk and priorities. Prevention involves organisational, technical, procedural, and personnel measures designed to reduce the likelihood of an incident. Preparedness primarily involves training, raising awareness, conducting drills and developing competencies.

Response involves the procedures to be followed should a threat materialise, whilst improvement involves analysing experiences, conducting audits, evaluating indicators, and implementing changes to the system. This framework represents an original synthesis of the logic found in risk management, occupational health and safety, and cybersecurity systems. This proposal is based on the principles of continuous improvement set out in ISO 45001 and ISO/IEC 27001, as well as the risk management functions defined in NIST CSF 2.0.

In the proposed approach, **people** take centre stage, whilst four key groups of tools operate around them: organisational solutions, procedural solutions, technical solutions and educational activities. Risk management, leadership and a safety culture should underpin the whole system, whilst the result of the system functioning correctly should be the protection of staff, the mitigation of risks arising from human factors and an increase in the organisation's resilience. This approach avoids the mistake of pitting employee safety against organisational safety. These are, in fact, two mutually complementary dimensions of the same system.

It can therefore be assumed that personnel safety management constitutes a purposeful, continuous and integrated process of identifying and mitigating threats to staff, developing their competence and awareness, controlling risks associated with access to resources, and preparing staff to respond to situations that disrupt the organisation's operations.

Its effectiveness depends not only on formal procedures and the technologies employed, but also on the quality of leadership, communication, safety culture and the genuine commitment of staff. Consequently, personnel safety must be regarded as an integral part of an organisation's safety management system, without which it is difficult to ensure the effective protection of its assets, maintain business continuity and build resilience to contemporary threats.

5. Conclusion

Staff safety is a key element of a modern organisational safety management system. The analysis carried out indicates that its significance extends beyond the traditional understanding of protecting employees' lives and health. Rapid technological, social and organisational changes are broadening the range of threats affecting staff, which now includes physical, psychosocial, organisational, information-related and cyber threats.

Consequently, effective safety management requires viewing the individual both as a person in need of protection and as an active participant in the safety system. The analysis carried out has demonstrated the dual nature of the human factor. On the one hand, an employee may be exposed to risks arising from the working environment, poor process organisation, violence, excessive workload, social engineering or cyber-attacks.

On the other hand, their decisions, behaviour, knowledge and level of awareness can directly influence the security of the entire organisation. Human error, failure to follow procedures or poor information management can lead to a serious incident, whilst a properly trained employee can recognise the signs of a threat and take action to mitigate its effects.

In response to the research question posed, how does personal security management affect the effectiveness of an organisation's security management system? – It must be concluded that this impact is both direct and multifaceted. Systematic personal safety management helps to reduce vulnerabilities arising from the human factor, raise awareness of risks, improve employees' preparedness to respond to incidents, protect key competencies and strengthen the organisation's ability to maintain business continuity. Personnel safety should therefore be treated as an integral part of organisational risk management, rather than as a separate area operating independently of the other components of the safety system.

The results of the analysis also provide positive confirmation of the research hypothesis. A systematic approach to personnel safety management – encompassing hazard identification, risk assessment, preventive measures, staff competence development, incident response and the refinement of existing solutions – can enhance the effectiveness of an organisation's safety system.

Of particular importance here is moving away from treating staff solely as a potential 'weak link'. Properly trained staff should be viewed as an active security asset, whose knowledge, experience and ability to identify threats can enhance the organisation's resilience.

Based on the above considerations, a model for an organisation's personnel security management system has been proposed, comprising six interrelated stages: identification, assessment, prevention, preparation, response and improvement. The central element of the model is the individual, whilst its operation is supported by organisational, procedural, technical and educational measures. The cyclical nature of the model implies that personnel safety cannot be built through isolated actions, but requires the continuous identification of changes occurring both within the organisation and in its environment.

Particular importance should be attached to the improvement stage in the proposed approach. Every incident, potentially hazardous event, audit result, exercise, or change in the nature of threats should provide information that enables a reassessment of risks and the modification of the safeguards in place. Consequently, the personnel security management system should be adaptive. This is particularly important in the context of the rapid development of digital technologies and artificial intelligence, as well as the evolution of social engineering methods, which give rise to new forms of influence on employees.

The practical significance of the approach presented lies in its applicability to organisations with diverse business profiles. The proposed model can serve as a basis for developing personnel security policies, planning training, identifying key posts, conducting risk assessments, managing access rights, and designing procedures for responding to crisis situations. It can also serve as a starting point for developing audit tools and metrics for the periodic assessment of personnel security levels.

At the same time, the analysis indicates the need for further empirical research. An interesting avenue would be to develop a tool to measure an organisation's maturity level in personnel security management and to investigate the relationships among security culture, staff awareness levels, incident frequency, and organisational resilience. Such research would enable empirical verification of the proposed model and the determination of the significance of its individual elements to the security system's effectiveness.

In summary, personnel safety should be treated as a strategic element of an organisation's safety management system. An effective organisation cannot limit itself to protecting infrastructure, information, and technical systems whilst neglecting the individual, who remains its user, operator, and decision-maker.

Integrating staff protection with risk management, safety culture, education, information security and business continuity helps to mitigate threats, whilst transforming the human factor into one of the fundamental resources that build an organisation's resilience. From this perspective, staff safety is not merely a cost or an organisational obligation, but an investment in the organisation's stability, continuity and ability to function in the face of current and future threats.

References:

Ani, U.D., He, H., Tiwari, A. 2019. Human Factor Security: Evaluating the Cybersecurity Capacity of the Industrial Workforce. Journal of Systems and Information Technology, 21(1), 2-35.

Bogusz, D. 2019. Spatial disorientation simulator. Safety & Defence – Scientific and Technical Journal, Volume 4, Issue 1.

Bogusz, D. 2021. Selection and Aviation Training of Military Pilots in the Polish Armed Forces. Military Aviation Academy Press, Dęblin.

Bogusz, D. 2024. Education and flight training of military pilots. Definitional issues. Journal of Modern Science, Volume 1/55/2024.

Bogusz, D. 2025. Flight simulators and training devices in the training of military pilots in Poland. LAW Publishing House, Dęblin.

Bogusz, D., Sidor, I. 2019. Training for staff handling dangerous goods in air transport. Maritime Safety Yearbook, Volume 13, Year XIII.

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

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

Ciekanowski, Z., Zurawski, S., Wysokinska, A., Kacprzak, A. 2025. The Role of a Leader in Shaping the Safety Culture of an Organisation. European Research Studies Journal, Vol. XXVIII, Issue 1, pp. 589-598.

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

Chodyka, M., Wojciechowska-Filipek, S., Ciekanowski, Z., Chrzaszcz, A., Zurawski, S. 2026. The Effectiveness of Security Management Systems in Public Organisations: A Cybersecurity Perspective. European Research Studies Journal, Vol. XXIX, Issue 1, pp. 478-489.

ENISA. 2018). Cyber Security Culture in Organisations. European Union Agency for Cybersecurity, Athens. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.

ENISA. 2019. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity.

ENISA. 2021. Raising Awareness of Cybersecurity, European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity.

ENISA. 2024. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

ENISA. 2025. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

Georgiadou, A., Mouzakitis, S., Askounis, D. 2022. A Cyber-Security Culture Framework for Assessing Organisation Readiness. Journal of Computer Information Systems, 62(3), 452-462.

Grudniewski, T., Ciekanowski, Z., Wolejszo, J., Mazur, S., Sobon, A., Kuznetsov, V. 2026. Cyber Threats to Public Administration as a Challenge to the Security of EU Countries. European Research Studies Journal, Vol. XXIX, Issue 2, pp. 606-615.

ILO. 2022. A Safe and Healthy Working Environment is a Fundamental Principle and Right at Work. International Labour Organisation, Geneva. https://www.ilo.org/topics-and-sectors/safety-and-health-work.

ILO. 2024. Preventing and Addressing Violence and Harassment in the World of Work through Occupational Safety and Health Measures. International Labour Organisation, Geneva. https://www.ilo.org/publications/preventing-and-addressing-violence-and-harassment-world-work-through.

ILO, Lloyd's Register Foundation, Gallup. 2022. Experiences of Violence and Harassment at Work: A Global First Survey. International Labour Organisation, Geneva. https://www.ilo.org/publications/major-publications/experiences-violence-and-harassment-work-global-first-survey.

Imam, A.H. 2023. Towards a Comprehensive Approach to Information Security Management: Empowering the Human Factor for Enhanced Security. International Journal of Computer Trends and Technology, 71(8), 1-11.

ISO (2018), ISO 45001:2018. Occupational Health and Safety Management Systems – Requirements with Guidance for Use. International Organisation for Standardisation, Geneva. https://www.iso.org/standard/63787.html.

ISO (2022), ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. International Organisation for Standardisation, Geneva. https://www.iso.org/standard/27001.

Khadka, K., Ullah, A. 2025. Human Factors in Cybersecurity: An Interdisciplinary Review and Framework Proposal. International Journal of Information Security, 24, Article 119. https://doi.org/10.1007/s10207-025-01032-0.

Larena-Luengo, A. et al. 2026. Influence of Human and Organisational Factors on Security Perception. International Journal of Information Security, 25, Article 106.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., Giannakopoulos, G. 2014. The Human Factor of Information Security: A Perspective on Unintentional Damage. Procedia – Social and Behavioural Sciences, 147, 424-428.

NIST. 2024. The NIST Cybersecurity Framework (CSF) 2.0,. National Institute of Standards and Technology, Gaithersburg, MD.

Pascoe, C., Quinn, S., Scarfone, K. 2024. The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Paper 29. National Institute of Standards and Technology.

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., Guerri, D. 2022. Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach. Cognition, Technology & Work, 24, 371-390.

Skóra, J., Bogusz, D. 2025. Contemporary Threats to National Security. Naval Academy Academic Press, Gdynia.

Verizon. 2025. 2025 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/.

Verizon. 2026. 2026 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/.

Yang, L., King, M., Yang, S.H. 2008. Integrating Technical Approaches, Organisational Issues, and Human Factors in Security Risk Assessment. In: Proceedings of the International Conference on Security and Cryptography – Secrypt, Insticc. https://www.scitepress.org/Papers/2008/17116/17116.pdf.