**Examining the Human Factors in Cybersecurity Practices: Psychological, Technical, and Organisational Perspectives**

**Abstract**. The study of human factors in cybersecurity is increasingly relevant due to the growing complexity and scale of cyber threats, coupled with the paradoxical position of humans as both a key element of protection and the most vulnerable link in information security systems. This study provides a comprehensive analysis of psychological, organisational, and technical aspects of human influence on cybersecurity and characterises strategies to minimise associated risks. The research employed systematic literature review, statistical assessment, comparison, systematic-logical methods, and generalization.

Key findings revealed important contradictions, including conflicts between system safety and usability, the challenge of balancing automation with human control, and ethical dilemmas related to employee monitoring. The research found that attackers actively exploit human psychological traits to gain unauthorised access, with techniques like "pretexting" becoming increasingly sophisticated. Special attention was given to incorporating human factors in security architecture design, which requires an interdisciplinary approach. User and Entity Behaviour Analytics (UEBA) systems enable detection of anomalous behaviours that may indicate insider activity, though careful configuration is needed to minimise false positives.

Literature analysis concluded that an integrated approach to cybersecurity must account for users' cognitive characteristics, organisational culture, and technological innovations. An effective cybersecurity strategy should incorporate personalised training programs, ergonomic security interfaces, and cybersecurity culture development across all organisational levels. Particular attention should focus on emotional intelligence and critical thinking to counter social engineering attacks.

These findings may benefit information security specialists, organisational leaders, security system developers, and researchers in psychology, organisational behaviour, and computer science.

Keywords: cybersecurity, security culture, social engineering, human factor, emotional intelligence, psychology

**Introduction**

Security in information and cyberspace has become increasingly vital amid the rapid digitalisation of all human activity domains [14, 17]. In the context of rapidly evolving information technologies, cybersecurity has become fundamental to organisational operations. However, despite implementing advanced technical solutions, the human factor remains a key component in protecting information systems. Consequently, many contemporary researchers focus on analysing the multifaceted impact of human factors on cybersecurity and developing strategies to minimise associated risks.

The problem of human error in cybersecurity refers to a variety of mistakes made by users rather than the failure of the computer, technology, or machine being used [15]. 74% of all data leaks are due to human error, according to the Infosec Institute report (Fig. 1).

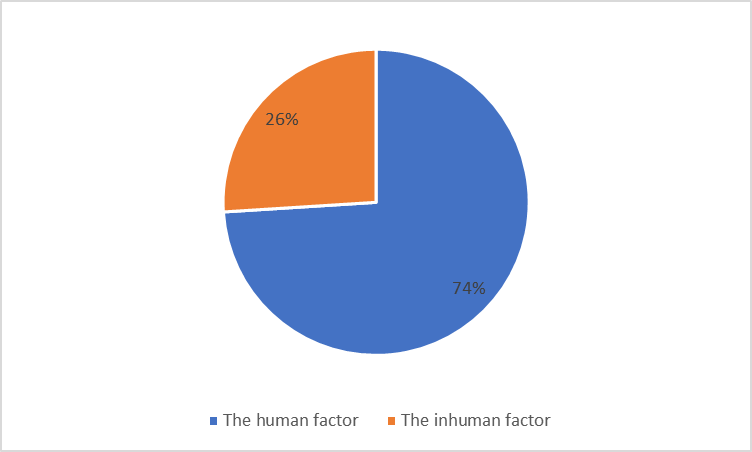


Fig. 1. Causes of data leaks [13]

The distribution presented in the chart underscores the critical vulnerability of information security to users’ behavioral and cognitive errors. The predominance of the human component in data breach mechanisms indicates the need to shift the focus toward the prevention of erroneous actions rooted in unawareness, inattentiveness, and social engineering. This, in turn, calls for the implementation of not only technical safeguards but also educational strategies for risk management.

The central problem of the study lies in the paradoxical position of the human factor in the cybersecurity system. On the one hand, humans serve as a critical element of information system protection, capable of adapting to new threats and making unconventional decisions. On the other hand, the human factor remains the most vulnerable link, often being the cause of serious security breaches. In simple words, the human interface is the target of semantic cyber-attacks, making them more serious than physical and syntactic cyber-attacks [16]. It is essential to address the following key issues: what are the main psychological mechanisms influencing user behavior in the context of cybersecurity; how can an understanding of the human factor be effectively integrated into the development of technical solutions and organizational security policies; and what strategies are most effective in minimizing risks associated with the human factor without compromising productivity and innovation.

**Methods and Materials**

This study employed a comprehensive interdisciplinary approach incorporating: systematic literature review (analysis of relevant scientific publications in cybersecurity, psychology, cognitive sciences, and organisational behaviour), statistical assessment, comparison, systematic-logical methods, and generalization.

Examination of modern scientific literature revealed several key research directions.

Particular attention is paid to the study of psychological and behavioural aspects of cybersecurity. A. Duzenci and co-authors investigate the influence of decision-making styles on adherence to cybersecurity protocols, emphasising the importance of an individualised approach to strategy development [4]. S. Nobles focuses on the issues of stress, burnout, and "security fatigue" in the context of cybersecurity, viewing them as problems of the human factor [9]. These studies highlight the need to consider the psychological state of employees when developing protective measures.

Organisational aspects are explored in the work of R.S. Dalal and co-authors, who note the abundance of research opportunities at the intersection of management science and cybersecurity [5]. C. Aksoy analyses the challenges of building a culture that enhances organisational resilience to cyberattacks, with a clear emphasis on the importance of a systematic approach to cybersecurity at the organisational level [1].

Educational aspects also draw researchers' attention. For instance, S.N. Sadiq Nasir examines the effectiveness of cybersecurity training programs, identifying success factors and best practices [10]. K. Amoresano and B. Yankson, using higher education as an example, characterise human errors as a critical factor contributing to data breaches [3]. These studies underscore the significant role of quality training and awareness-raising in the field of cybersecurity.

An interesting interdisciplinary approach is presented in the study by Sh.L. Burton and co-authors, who examine the relationship between leadership in cybersecurity, human factors, emotional intelligence, and innovative behavior. This approach demonstrates the complexity and multidimensionality of the problem under investigation [4].

Ethical aspects are described and evaluated in the publication by J. Fenech and co-authors, who explore the role of relevant principles in shaping value-oriented decision-making in the field of cybersecurity [7]. Emphasis is placed on the importance of the ethical dimension in strategies.

Technological aspects and their interaction with the human factor are also reflected in contemporary literature. For example, M.J.H. Aljrad and K. Al-Dhlan study the nuances of the impact of social engineering on cybersecurity in the Internet of Things environment, illustrating how technological innovations create new challenges [2].

Particular attention should be given to the work of M. Vuković and T. Štefanac—the authors consider cybersecurity and human factor issues through the lens of digital cultural heritage [12].

Statistical data on phishing attacks, provided by G. Smith, complement the overall picture by offering a quantitative assessment of the scale of the problem, confirming the relevance of research regarding the role of the human factor in ensuring and maintaining cybersecurity [11].

Thus, modern authors emphasise the interdisciplinary nature of the discussed issue, covering psychological, organisational, educational, ethical, and technological aspects. There is a noticeable trend toward integrating various approaches to create comprehensive cybersecurity strategies that take into account the complexity and multifaceted nature of the human factor.

To achieve the objectives of this study, a systematic interdisciplinary approach was employed, involving a comprehensive analysis of scholarly publications spanning adjacent fields — cybersecurity, psychology, cognitive science, behavioral economics, organizational studies, and applied ethics. The foundation of this work is a systematic literature review, implemented through a multi-stage procedure encompassing the search, selection, categorization, and synthesis of relevant sources.

At the initial stage, a targeted search for academic articles published over the past ten years in peer-reviewed journals and proceedings of international conferences was conducted. Search queries were constructed based on key concepts and executed using academic databases.

Following the preliminary selection based on thematic relevance, the sources underwent content-driven analytical screening: publications with insufficient scientific validity were excluded, as were works limited to purely technical or regulatory perspectives without consideration of behavioral or organizational dimensions. The synthesis phase involved the application of a systematic-logical method, enabling the identification of principal research directions: psychological and behavioral determinants, organizational prerequisites, educational models, ethical dilemmas, and technological challenges. Each thematic category was derived from recurring focal points and conceptual intersections identified within the selected body of literature.

Cross-disciplinary linkages were revealed, highlighting a discernible trend toward the integration of diverse approaches and the emergence of multi-level cybersecurity strategies. The inclusion of empirical data — both in the form of quantitative statistics (e.g., phishing prevalence) and qualitative case studies — ensured the robustness and validity of the conclusions drawn.

Thus, the selection and processing of sources were aimed not merely at capturing the current state of academic discourse, but also at constructing a coherent analytical framework that reflects the complexity and multidimensionality of the issue under investigation.

**Results and Discussion**

The examination of the human factor issue should begin with the characterisation of psychological aspects of cybersecurity. Cognitive characteristics of individuals play a significant role in their behaviour in the digital environment. The phenomenon of "change blindness" may lead employees to overlook subtle but critical changes in program interfaces, potentially exposing them to phishing attacks. The Dunning-Kruger effect, where individuals overestimate their skills, often results in neglecting basic information hygiene rules. The Dunning-Kruger effect is a cognitive bias in which people with low ability, knowledge, or competence in a particular area tend to overestimate their abilities. This phenomenon was first identified by psychologists David Dunning and Justin Kruger in 1999. It suggests that individuals who lack expertise in a subject often do not realise their deficiencies, leading to inflated self-assessments.

Impulsiveness and risk-taking tendencies, typical for certain personality types, may manifest in the hasty opening of suspicious attachments or clicking on dubious links. Conversely, excessive caution can sometimes paralyse work processes, reducing organisational efficiency.

Next, attention should be given to social engineering manipulation features (Table 1).

Table 1 – Social Engineering in the Context of Human Factors in Cybersecurity

(compiled by the author based on [2, 6, 8])

|  |  |
| --- | --- |
| **Situation** | **Description** |
| Phishing | Fraudulent emails and messages |
| Data extraction | Attacks through phone calls or social networks |
| Exploitation of trust | Abuse of trusted relationships within a company |

Three typical scenarios can thus be identified—phishing, data extraction, and exploitation of trust—each characterized by manipulative influence on user behavior. Phishing is defined as distributing fraudulent messages aimed at deceiving victims to obtain confidential information. Data extraction refers to attacks via phone calls or social networks, highlighting multi-channel formats’ in social engineering tactics. Exploitation of trust points to internal corporate communications' vulnerability, where malicious actors leverage existing employee relationships to gain system access.

Attackers actively exploit human psychological traits to gain unauthorised access to information. The technique of "pretexting," where the attacker creates a plausible scenario to manipulate the victim, is becoming increasingly sophisticated. Phishing campaigns employing social engineering methods are evolving, adapting to the growing awareness of users. According to "DMARC" data, in 2022, the highest number of phishing attacks occurred in the Netherlands (17.7% of the total), followed by Russia, Moldova, the USA, and Thailand [11] (Fig. 2).



Fig. 2. Statistical data on phishing cases [11]

This distribution points to concentrated vulnerabilities in specific national infrastructures or user behavior patterns, highlighting the need for regionally tailored cybersecurity policies and awareness programs.

The phenomenon of "clickbait" in the context of cybersecurity is gaining new significance: provocative headlines and images are not only used to attract attention but also to spread malware. Exploiting a sense of urgency and the fear of missing out has become a powerful tool in the hands of cybercriminals.

Focus must be given to the role of the human factor in security architecture. Designing such systems with this factor in mind requires an interdisciplinary approach. The concept of "security through inconvenience" is gradually giving way to more ergonomic solutions [5]. The implementation of biometric authentication systems reduces the cognitive load on users, minimising risks associated with password management.

The principle of least privilege, when properly implemented, reduces the potential damage from human errors. However, its implementation relies on meticulous fine-tuning and requires constant monitoring.

The development of a cybersecurity culture is a process that requires a systematic approach. Traditional methods of employee training are being replaced by gamified platforms and simulations of real attacks. The concept of "ethical phishing" helps identify weak points within the organisation and work strategically to enhance its resilience to social engineering attacks.

The practice of implementing "security champions"—employees acting as cybersecurity ambassadors within their departments—contributes to the organic spread of a security culture [11]. This approach helps bridge the gap between technical specialists and regular users.

High levels of stress and chronic fatigue among employees can significantly reduce the effectiveness of cybersecurity measures. The phenomenon of "security fatigue" manifests as neglect of basic rules due to cognitive overload. In this context, the development of ergonomic interfaces and procedures that minimise cognitive strain on users is crucial.

The concept of "microlearning" in cybersecurity helps maintain a high level of staff awareness without significant time investment. Short but regular training sessions help to form stable patterns of safe behaviour in the digital environment.

Insider threat issues require a comprehensive approach accounting for both technical and psychological aspects (Table 2). Analysing potential insiders' motivation allows for developing effective prevention strategies. In this context, the "zero trust" concept becomes particularly significant, minimising risks associated with trust abuse.

Table 2 – Variants of insider threats (compiled by the author based on [1, 4, 12])

|  |  |
| --- | --- |
| **Variant** | **Description** |
| Malicious employees | Intentional actions by employees to steal data |
| Unintentional actions | Employee mistakes leading to information leaks |
| Employee turnover | Risks associated with the departure of employees who have access to confidential information |

Implementing User and Entity Behaviour Analytics (UEBA) systems enables detection of anomalous user behaviour patterns that may indicate insider activity. However, the application of such systems requires careful configuration to minimise false positives.

The effectiveness of incident response in cybersecurity largely depends on the human factor. The phenomenon of "hindsight bias" often distorts the assessment of an incident and complicates the extraction of relevant lessons.

Several conceptual developments in this field focus on enhancing the adaptive capabilities of both the system and personnel. This includes not only technical training but also the development of "soft" skills—critical thinking and the ability to make decisions under uncertainty.

The analysis of the role of the human factor in ensuring cybersecurity opens broad prospects for further research. Below are the key recommended directions that require in-depth study (Table 3):

Table 3 – Recommendations for future research (compiled by the author)

|  |  |
| --- | --- |
| **Direction** | **Description** |
| 1. Neurocognitive mechanisms of decision-making in the context of cybersecurity | Research into the neural correlates of risk assessment when interacting with potentially dangerous content. Study of the influence of stress on prefrontal cortex activity and its connection to decision-making in information security. |
| 2. Cross-cultural aspects of cybersecurity threat perception | Comparative analysis of attitudes toward privacy and security in various cultural contexts. Development of culturally adapted cybersecurity training strategies. |
| 3. Long-term effects of gamification in cybersecurity training | Longitudinal studies on the effectiveness of gamified approaches in forming stable patterns of safe behaviour. Evaluation of skill transfer from game scenarios to real-life situations. |
| 4. Integration of behavioral economics into security system design | Application of nudge theory concepts to optimise the user interface of security systems. Study of the influence of choice architecture on cybersecurity decision-making. |
| 5. Psycholinguistic analysis of phishing messages | Development of machine learning algorithms to identify linguistic markers characteristic of social engineering attacks. Investigation of the effectiveness of various linguistic strategies in the context of targeted phishing. |
| 6. Influence of emotional intelligence on resistance to social engineering attacks | Study of the correlation between emotional intelligence levels and the ability to recognise manipulative techniques. Development of methods to enhance emotional intelligence in the context of cybersecurity. |
| 7. Ethical aspects of employee monitoring | Examination of the balance between security and privacy in the corporate environment. Development of ethical frameworks for the implementation of behavioural analytics systems. |
| 8. Cognitive ergonomics of security interfaces | Optimisation of authentication system design with consideration of user cognitive load. Study of the influence of visual and auditory cues on threat perception and decision-making. |
| 9. Psychological aspects of rehabilitation after cyber incidents | Study of the long-term psychological consequences for victims of cyberattacks. Development of support and rehabilitation programs for employees who made critical security errors. |
| 10. Application of complex systems theory to the analysis of the human factor in cybersecurity | Modelling the interaction between technical and human components of the security system using dynamic systems theory. Identification of bifurcation points in user behaviour for the development of preventive measures. |

An in-depth exploration of the described research directions will significantly enhance the understanding of the human factor's role in ensuring cybersecurity and contribute to the development of more effective strategies for protecting information systems. An interdisciplinary approach that integrates advances in psychology, neuroscience, linguistics, and computer science appears to be the most promising for addressing the complex problems in this field.

**Conclusions**

The human factor remains both the most vulnerable and the most adaptable element in cybersecurity systems. A full and correct understanding of psychological mechanisms underlying user behaviour enables development of more effective protection strategies.

The integration of technical solutions accounting for human cognitive characteristics and cybersecurity culture formation are key factors in building resilient information security systems. Ultimately, the synergy between technological innovations and development of human potential will determine success in countering the ever-evolving cyber threats.

COMPETING INTERESTS:

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

**References**

1. Aksoy C. Building a cyber security culture for resilient organizations against cyber-attacks / C. Aksoy // Journal of Business Economics and Management Research. – 2024. – Vol. 7. – No. 1. – Pp. 96-110.

2. Aljrad M.J.H. The effect of using social engineering for cybersecurity on the Internet of things environment / M.J.H. Aljrad, K. Al-Dhlan // Journal of Science and Technology. – 2023. – Vol. 27. – No. 2. – Pp. 43-47.

3. Amoresano K. Human error – a critical contributing factor to the rise in data breaches: a case study of higher education / K. Amoresano, B. Yankson // HOLISTICA – Journal of Business and Public Administration. – 2023. – Vol. 14. – No. 1. – Pp. 110-132.

4. Burton Sh.L. Exploring the nexus of cybersecurity leadership, human factors, emotional intelligence, innovative work behavior, and critical leadership traits / Sh.L. Burton, D.N. Burrell, C. Nobles, L.A. Jones // Scientific Bulletin. – 2023. – Vol. 28. – No. 2. – Pp. 162-175.

5. Dalal R.S. Organizational science and cybersecurity: abundant opportunities for research at the interface / R.S. Dalal, D.J. Howard, R.J. Bennett, C. Posey, S.J. Zaccaro, B.J. Brummel // Journal of Business and Psychology. – 2022. – Vol. 37. – No. 1. – Pp. 1-29.

6. Duzenci A. The role of decision-making styles in shaping cybersecurity compliance behavior / A. Duzenci, H. Kitapci, M.S. Gok // Applied Sciences (Switzerland). – 2023. – Vol. 13. – No. 15. – Pp. 87-91.

7. Fenech J. Ethical principles shaping values-based cybersecurity decision-making / J. Fenech, D. Richards, P. Formosa // Computers & Security. – 2024. – Vol. 140. – Pp. 103-115.

8. Kraus K. Digital professions of the future: what changes to expect to human capital in the conditions of establishing social entrepreneurship? / K. Kraus, N. Kraus, O. Marchenko // Innovation and Sustainability. – 2022. – No. 1. – Pp. 53-64.

9. Nobles C. Stress, burnout, and security fatigue in cybersecurity: a human factors problem / C. Nobles // HOLISTICA – Journal of Business and Public Administration. – 2022. – Vol. 13. – No. 1. – Pp. 49-72.

10. Sadiq Nasir S.N. Exploring the effectiveness of cybersecurity training programs: factors, best practices, and future directions / S.N. Sadiq Nasir // Advances in Multidisciplinary and scientific Research Journal Publication. – 2023. – Vol. 2. – No. 1. – Pp. 151-160.

11. Smith G. Top Phishing Statistics for 2024: Latest Figures and Trends / G. Smith // URL: <https://www.stationx.net/phishing-statistics/> (date of application: 09/19/2024).

12. Vuković M. Digital cultural heritage, cybersecurity, and the human factor / M. Vuković, T. Štefanac // Preservation, Digital Technology and Culture. – 2023. – Vol. 52. – No. 4. – Pp. 129-141.

13. Peters J. Human error is responsible for 74% of data breaches / J. Peters // URL: https://www.infosecinstitute.com/resources/security-awareness/human-error-responsible-data-breaches/ (date of application: 09/19/2024).

14. Loishyn AA, Hohoniants S, YaTkach M, Tyshchenko MH, Tarasenko NM, Kyvliuk VS. Development of the Concept of Cybersecurity of the Organization. TEM Journal. 2021 Aug 1;10(3):1447.

15. Amoresano K, Yankson B. Human error-A critical contributing factor to the rise in data breaches: A case study of higher education. Holistica Journal of Business and Public Administration. 2023;14(1):110-32.

16. Tikanmäki I, Ruoslahti H. Insights on Human Factors Enhancing Cybersecurity. Information & Security. 2024;55(3):225-35.

17. Okoro DC. An Evaluation of Cybersecurity Frameworks and Privacy Regulations for Companies in the Digital Age: A Legal Approach. Asian J. Econ. Busin. Acc. 2025 Apr. 12;25(4):431-40.