Human Factors in Cybersecurity, Vol. 208, 2026, 64–74
https://doi.org/10.54941/ahfe1007413

Governing the Human Factor in Cybersecurity: A Regulatory Perspective

Dusko Milojevic, Jan De Bruyne, and Maja Nisevic

Centre for IT & IP Law (CiTiP), KU Leuven, Leuven, Belgium

ABSTRACT

In an increasingly interconnected world, cyberattacks have emerged as one of the most pressing global threats, endangering critical infrastructure, compromising sensitive data, and disrupting essential services across sectors. As a result, cybersecurity has become a key policy priority at all levels of governance. In response, the European Union (EU) adopted, inter alia, the Cybersecurity Strategy for the Digital Decade and significantly expanded its legislative framework to strengthen cybersecurity requirements through both horizontal and sector-specific regulatory instruments. Alongside policy instruments, cybersecurity efforts have emphasised technical measures to address the evolving cybersecurity threat landscape. However, there is growing recognition that cybersecurity cannot be effectively understood or addressed solely through technical measures. Cybersecurity posture depends not only on technological safeguards but also, fundamentally, on the so-called 'human factor'. Against this backdrop, this article examines how the human factor is conceptualised and addressed within the EU's cybersecurity legal frameworks. Adopting a qualitative, interdisciplinary approach grounded in doctrinal legal research, the article analyses the regulatory treatment of the human factor within EU cybersecurity law. It contributes to broader debates on cybersecurity governance by identifying regulatory gaps, proposing recommendations for better integrating human-centred cybersecurity strategies into EU regulatory frameworks, and outlining avenues for future research to strengthen cybersecurity resilience.

Keywords: Human factor, Cybersecurity, Regulatory governance

INTRODUCTION

Over the past decade, digital transformation has accelerated across sectors, with emerging technologies such as surgical robotics, autonomous systems, and quantum computing increasingly shaping critical infrastructures and everyday practices (Gharib & Gahi, 2025; Mahmood, 2024). However, alongside these transformative innovations come significant societal challenges, with cybersecurity standing out as one of the most critical and urgent concerns. Successful cyberattacks may impede critical sector operations, lead to the loss of sensitive data, compromise safety, cause reputational harm and financial losses, and, in extreme cases, lead to loss of life (ENISA, 2025; Milojevic & Nisevic, 2024). Hence, many renowned reports, such as the World Economic Forum Global Risks Report (2025), identify cyberattacks as a substantial global risk.

Received February 6, 2026; Revised April 10, 2026; Accepted April 24, 2026; Available online July 20, 2026

Consequently, cybersecurity has become a key policy priority at all levels of governance. The EU adopted the Cybersecurity Strategy for the Digital Decade to strengthen the EU's cybersecurity posture as a policy response to mitigate cybersecurity challenges. Furthermore, the EU legislative framework has undergone significant changes to enhance cybersecurity requirements, encompassing horizontal and sector-specific legislation, such as the Network and Information Systems Directive (NIS2), the Cybersecurity Act (CSA), the General Data Protection Regulation (GDPR), the Artificial Intelligence Act (AI Act), and the Medical Devices Regulation (MDR). Alongside policy instruments, cybersecurity efforts have predominantly focused on technical solutions to address the evolving cybersecurity threat landscape (Malatji et al., 2020; Kumar et al., 2021; Thomasian & Adashi, 2021; Zhang et al., 2022). Information security efforts have traditionally emphasised technical measures, such as firewalls, intrusion detection systems, and robust authentication protocols, to strengthen cybersecurity posture (Thomasian & Adashi, 2021).

Yet, despite the above-mentioned policy initiatives and technical safeguards, cyberattacks continue to grow in frequency and severity, with recent data indicating substantial financial impacts on critical infrastructure sectors (Annual Data Breach Report, 2024; ENISA, 2025). While recent data underline the severity of cybersecurity threats, there is growing recognition that cybersecurity posture depends not only on technical measures but fundamentally on addressing the so-called 'human factor' as a core element of cybersecurity (Morgan et al., 2020). In other words, even though technical countermeasures are in place, the human factor remains a key challenge in information security (Rohan et al., 2023). Consequently, there is a growing assertion that cybersecurity can no longer be reduced to the mere technical protection goals of IT security (Veale & Brown, 2020). It has progressively developed into a multidisciplinary challenge (Chiara, 2022), necessitating further research of the human role in cybersecurity (Colabianchi et al., 2025).

Accordingly, this article examines how current EU cybersecurity regulations, such as the NIS2, CSA, GDPR, MDR, and the AI Act, govern the human factor in cybersecurity. In addition, the article also aims to contribute to the broader understanding of cybersecurity governance by moving beyond a purely technical perspective, focusing on how the human factor is addressed within the EU's legal frameworks. Therefore, it will provide a brief overview of the previous work in the field, pointing out challenges surrounding the human factor. Then it will position the human factor within the broader cybersecurity landscape, analysing governance. Finally, the article proposes recommendations for better integrating human-centred cybersecurity strategies into EU regulatory frameworks and outlines a research agenda for future research on strengthening cybersecurity resilience. Methodologically, the article adopts a qualitative and interdisciplinary approach, grounded in doctrinal legal analysis of EU cybersecurity law. It examines the interpretation, interaction, and coherence of horizontal and sector-specific EU legal instruments, informed by insights from cybersecurity governance and human-centric security scholarship.

UMAN FACTOR IN CYBERSECURITY: BACKGROUND AND LITERATURE OVERVIEW

Humans are often perceived as the weakest link in the cybersecurity chain (Cartwright, 2023; Yeng et al., 2019), and the most significant vulnerability (Ahmadi et al., 2024; Triplett, 2022). A growing body of literature, policy papers, and reports highlights humans as the biggest challenge in ensuring robust cybersecurity protection (Gadge et al., 2024; Verhulsdonck et al., 2023). For instance, Verizon's report revealed that the human factor contributed to approximately 68% of breaches in 2024, and remained almost the same in 2025 (Data Breach Investigations Report, 2024, 2025). In the same vein, Thales's report, which reflects insights from 18 countries across 37 industries, emphasises that internal human error remains a critical threat area. It points out that human error consistently ranks highly, if not the top threat category, and reports that human factor is still a major cause of cloud data breaches (Data Threat Report: Navigating New Threats and Overcoming Old Challenges, 2024). The European Union Agency for Cybersecurity (ENISA), through its various reports, emphasises the critical role of humans in the cybersecurity landscape. For instance, ENISA highlights human error as a persistent and growing threat, warning that its impact is expected to become even more pronounced in the future (Report on the State of Cybersecurity in the Union, 2024).

Prior studies have predominantly emphasised technological solutions, often neglecting the pivotal role of the human factor in maintaining cybersecurity (Delso-Vicente et al., 2025). As human-related cybersecurity risks have increasingly been recognised as comparable in significance to technical vulnerabilities, research has gradually shifted towards greater attention to the human factor (Jeong et al., 2019). However, scholarship in this area remains limited, with human-centric approaches still underrepresented in cybersecurity governance and academic discourse (AL-Nuaimi, 2024; Nobles, 2018). This ongoing oversight signals a continued neglect of the human layer in shaping secure systems. While this body of literature convincingly demonstrates the scale of human-related cybersecurity incidents, it also reveals a tendency to frame humans primarily as liabilities, rather than as integral components of socio-technical systems shaped by organisational, regulatory, and governance choices.

CONCEPTUAL AND TERMINOLOGICAL AMBIGUITY

The humans in the cybersecurity ecosystem are colloquially encapsulated by the umbrella term "human factor". However, the "human factor" concept in scholarly literature often remains undefined and open to varied interpretations. The pervasive absence of conceptual and terminological clarity is a fundamental challenge in human-centric cybersecurity research. Terms such as "human element," "human dimension," "insider threat," "end-user," and "human resources security" are frequently used across the literature to refer, often interchangeably and inconsistently, to what is broadly understood as the human factor in cybersecurity (AL-Nuaimi, 2024; Georgiadou et al., 2022; Jeong et al., 2019; Nobles, 2018; Sari et al., 2022). This ambiguity extends to authoritative reports. For instance, ENISA

employs terms like the "human dimension" without clear definitions (ENISA, 2020). This conceptual uncertainty significantly undermines the coherence of the field. Accordingly, whether the "human factor" refers to individual traits, organisational dynamics, or systemic issues remains critically unclear. Moreover, conceptual ambiguity is not merely an academic concern.

From a regulatory perspective, it directly affects the design, interpretation, and implementation of legal obligations, as unclear conceptualisations of the human factor translate into vague or under-specified regulatory expectations. More precisely, while the NIS2 acknowledges the human factor (Recital 78), it provides no definition. Similarly, the CSA also acknowledges importance of human factor. The CSA Recital 8 points out that cybersecurity is not only an issue related to technology, but one where human behaviour is equally important. Unlike the NIS2, the CSA uses formulation "human behaviour". However, as the CSA does not provide any further reference to either human behaviour, nor human factor and it remains unclear whether the CSA refers to individual human traits, or humans in general, as part of organisational setting. The absence of clear definitions creates a significant risk of legal uncertainty and inconsistent compliance. Without conceptual precision, establishing effective cybersecurity governance becomes inherently difficult. This fragmentation emphasises the urgent need for a more precise, legally grounded conceptualisation of the meaning of the human factor in cybersecurity.

BEHAVIOURAL SCIENCE AND INSIDER THREAT APPROACHES: A FRAGMENTED LANDSCAPE

While the technical focus still predominantly occupies the research domain (Jeong et al., 2019), the scarce body of literature observes the human element through the behavioural science lenses. Behavioural science literature on cybersecurity primarily focuses on individual attributes, such as gender (Anwar et al., 2017; Neupane et al., 2016), age (Farooq et al., 2015; Ki-Aries & Faily, 2017), personality and cultural context (Henshel et al., 2016; Luo et al., 2011), cognitive load and bias (Pfleeger & Caputo, 2012). While the observation of isolated personal traits provides nuanced insights into human behavior towards cybersecurity, some scholars argue that these aspects cannot be fully comprehended in isolation and call for a more comprehensive approach (Jeong et al., 2019). Focusing narrowly on isolated behavioural traits neglects broader systemic and contextual realities that profoundly influence human vulnerabilities, such as staff and skill shortages, limited budgets, and diverse attack vectors (Brilingaitė et al., 2024; Malatji et al., 2020; Morgan et al., 2020). Furthermore, these studies frequently suffer from limited sample sizes, a narrow focus, and a lack of generalizability, hindering the development of actionable, governance-oriented recommendations. This highlights a fragmented research agenda that struggles with integrating individual and systemic factors.

Another body of literature observes humans as an "insider threat", differentiating between "malicious insider" and "accidental/unintentional human error", the former receiving more scholarly attention (Evans et al., 2019). In contrast, unintentional human errors, such as using poor password practices and susceptibility to phishing emails, are far more common yet

receive significantly less attention (Hadlington, 2018). While malicious insiders have received more attention, it is interesting to note that widely cited reports, such as previously cited Verizon's report, found that these threats are significantly lower than those of unintentional human error. Some scholars also argue that the concept of "insider threat" in the context of cyber systems has proven problematic, as there is considerable disagreement surrounding the definition of what constitutes an insider threat (Bishop & Gates, 2008). Similarly, ENISA's threat landscape reports also acknowledge this issue and do not include the insider threat actor as one of the primary threat actors in their reports, due to the very low number of public reports of incidents (ENISA, 2024). This narrow focus on rare but dramatic threats inadvertently ignores the everyday realities of human error as a critical and pervasive vulnerability.

In summary, research on human behavior, error, and insider threats remains narrow and fragmented (Colabianchi et al., 2025; Morgan et al., 2020; Nobles, 2018; Rahman et al., 2021). Crucially, critical vectors for cyber risks linked to the human factor remain understudied (Rahman et al., 2021). Consequently, scholars are pointing out that it is essential to better understand the human factor and cybersecurity risks, threats, and vulnerabilities (AL-Nuaimi, 2024; Morgan et al., 2020). This highlights the need for integrative, interdisciplinary research to develop a more comprehensive, human-centric cybersecurity governance model. Taken together, this body of scholarship demonstrates that while the human factor is increasingly recognised as critical to cybersecurity, existing research has largely focused on individual behaviour and technical controls, with comparatively limited attention paid to the role of regulatory governance in structuring organisational practices and shaping human-related cybersecurity risks.

POSITIONING THE HUMAN FACTOR IN THE EU CYBERSECURITY LEGAL FRAMEWORK

The EU regulatory cybersecurity landscape evolves at a fast pace, encompassing both horizontal and sector-specific legislation. Some of the central pieces of the EU cybersecurity regulatory architecture that contain rules targeting humans are the NIS2, the CSA, the GDPR, the MDR, and the AI Act. These frameworks address the human factor to varying extents, mostly through the risk management measures. The NIS2 is the only regulatory framework that explicitly addresses humans through several recitals and articles. For instance, Article 21 of the NIS2 mandates that risk management measures will include, inter alia, at least "cybersecurity training" (Article 21(2)(g)) and "human resources security" (Article 21(2)(i)). However, NIS2 does not provide any further clarification on what "human resources security" measures should entail.

On the other hand, while cybersecurity training is a self-explanatory measure, scholars are pointing out its limitations in building a cybersecurity posture. More specifically, training alone cannot mitigate cybersecurity threats caused by humans (Morgan et al., 2020), and the human factor is much more comprehensive than a security awareness program (Robinson, 2023). Additionally, in accordance with the NIS2 Article 20(2), Member States shall ensure that "members of the management bodies of essential

and important entities must attend training" and shall encourage essential and important entities to regularly offer similar training to their employees. Hence, NIS2 imposes an obligation on the top-level management of essential and important entities that must attend training, whereas this approach to lower organisational layers is at the level of recommendation, but not an obligation. As such, Member States may adopt different approaches to this measure, thus leading to a diverging approach to NIS2 implementation, and, eventually, undermining harmonization efforts to build a common level of cybersecurity across the Union.

Furthermore, the GDPR, the MDR, and the AI Act do not explicitly refer to the human factor. An implicit reference to humans in these regulations can be found in the legal requirement "to establish appropriate technical and organisational measures proportional to the data processing risk". While humans should be addressed through "organisational measures", these regulations mostly provide examples of technical measures, thus failing to acknowledge the importance of the human factor. This regulatory silence on the role of humans creates ambiguity in implementation and weakens the human-centric cybersecurity posture. Accordingly, there is a pressing need for a more coherent legal approach that explicitly incorporates and operationalizes the role of humans in cybersecurity governance, moving beyond general obligations. Taken together, these instruments point to a regulatory pattern in which the human factor is addressed mainly through abstract organisational obligations, while lacking clear conceptualisation and operationalisation, thereby contributing to fragmented and uneven implementation across Member States.

WAY FORWARD

Looking forward, strengthening cybersecurity resilience in the EU requires a more explicit and coherent integration of the human factor into cybersecurity regulation and policy frameworks. This does not entail replacing technical safeguards, but rather complementing them with clearer legal expectations regarding human-centric risk management, organisational responsibility, and governance design. Regulatory guidance, supervisory practices, and standard-setting processes offer important avenues for operationalising the human factor in a manner that is consistent across sectors and Member States.

Future research should further explore how human-centric cybersecurity principles can be embedded into regulatory frameworks, including through comparative analysis of national implementation practices and closer engagement with organisational and behavioural scholarship.

CONCLUSION

This article briefly examined how the human factor is conceptualised and addressed within the EU's cybersecurity legal framework, with the aim of moving beyond a predominantly technical understanding of cybersecurity governance. By analysing the interaction between key EU regulatory instruments and existing human-factor scholarship, the article has demonstrated that although the importance of human-related cybersecurity

risks is increasingly recognised, regulatory governance remains an underdeveloped dimension in both academic research and legal design.

The analysis revealed a persistent regulatory pattern in which the human factor is acknowledged indirectly through general organisational obligations and risk management requirements, yet remains insufficiently conceptualised and operationalised. While NIS2 introduces explicit references to cybersecurity training and human resources security, it provides limited guidance on the scope and content of such measures. Other central instruments, including the GDPR, the AI Act, the MDR, and the CSA, rely primarily on broadly framed organisational measures that implicitly encompass human-related risks but predominantly prioritise technical safeguards. As a result, regulatory expectations concerning the human factor remain fragmented and open to divergent interpretation, contributing to uneven implementation across Member States.

These findings point to a broader governance challenge. Framing the human factor primarily through abstract compliance obligations or isolated training requirements risks reinforcing a narrow understanding of human-related cybersecurity risks, detached from organisational structures, regulatory incentives, and systemic conditions shaping human behaviour. Without clearer regulatory articulation, legal frameworks struggle to translate insights from behavioural and socio-technical research into coherent and actionable governance requirements. This gap helps explain why human-related vulnerabilities persist despite increasing regulatory activity and technological investment.

By foregrounding regulatory governance as a central dimension of the human factor, this article contributes to ongoing debates on the evolution of EU cybersecurity law and highlights the need for a more integrated approach capable of addressing the socio-technical, multidimensional, and interdisciplinary nature of cybersecurity in an increasingly complex digital environment.

ACKNOWLEDGMENT

This research was supported by the PERUN project (Protecting Sensitive Cyber Ecosystems from Upcoming Next Generation and AI-generated Malware Threats), funded by the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101225653.

REFERENCES

Ahmadi, M., Ramezankhani, M., Kakavand, M., & Tahir, M. (2024). Analyzing the Correlation Between Employee Security Awareness and Cyberattack Vulnerability: A Quantitative Study. In K. Arai (Ed.), Proceedings of the Future Technologies Conference (FTC) 2024, Volume 4 (pp. 195–211). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-73128-0_13

AL-Nuaimi, M. N. (2024). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: A systematic review. Global Knowledge, Memory and Communication, 73(1/2), 1–23. https://doi.org/10.1108/GKMC-12-2021-0209

Alohali, M., Clarke, N., Furnell, S., & Albakri, S. (2017). Information security behavior: Recognizing the influencers. In 2017 Computing Conference (pp. 844–853). IEEE.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Bishop, M., & Gates, C. (2008). Defining the insider threat. Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, 1–3. https://doi.org/10.1145/1413140.1413158

Brilingaitė, A., Bukauskas, L., Domarkienė, I., Rančelis, T., Ambrozaitytė, L., Pirta-Dreimane, R., Lugo, R. G., & Knox, B. J. (2024). Towards Projection of the Individualised Risk Assessment for the Cybersecurity Workforce (SSRN Scholarly Paper No. 4807481). Social Science Research Network. https://doi.org/10.2139/ssrn.4807481

Cartwright, A. J. (2023). The elephant in the room: Cybersecurity in healthcare. Journal of Clinical Monitoring and Computing, 1–10. https://doi.org/10.1007/s10877-023-01013-5

Chiara, P. G. (2022). The Cyber Resilience Act: The EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. International Cybersecurity Law Review, 3(2), 255–272. https://doi.org/10.1365/s43439-022-00067-6

Colabianchi, S., Costantino, F., Nonino, F., & Palombi, G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. Journal of Innovation & Knowledge, 10(3), 100695. https://doi.org/10.1016/j.jik.2025.100695

Delso-Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O., & de Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: A systematic literature review of behavioral and technological aspects in cybersecurity. Future Business Journal, 11(1), 28. https://doi.org/10.1186/s43093-025-00452-7

European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2020). The EU's cybersecurity strategy for the digital decade (JOIN(2020) 18 final).

European Union Agency for Cybersecurity (ENISA). (2020). Research topics: ENISA Threat Landscape.

European Union Agency for Cybersecurity (ENISA). (2024). *Report on the state of cybersecurity in the Union.*

European Union Agency for Cybersecurity (ENISA). (2024) ENISA Threat Landscape 2024.

European Union Agency for Cybersecurity (ENISA). (2025). ENISA threat landscape 2025.

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.

European Union. (2017). Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009, and repealing Council Directives 90/385/EEC and 93/42/EEC (Medical Devices Regulation). Official Journal of the European Union, L 117, 1–175.

European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, 15–69.

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union, L 1689.

Evans, M., He, Y., Maglaras, L., Yevseyeva, I., & Janicke, H. (2019). Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. International Journal of Medical Informatics, 127, 109–119. https://doi.org/10.1016/j.ijmedinf.2019.04.019

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. 2015 IEEE Trustcom/BigDataSE/ISPA, 1, 352–359. https://doi.org/10.1109/Trustcom.2015.394

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting Insider Threat via a Cyber-Security Culture Framework. Journal of Computer Information Systems, 62(4), 706–716. https://doi.org/10.1080/08874417.2021.1903367

Gharib, J., & Gahi, Y. (2025). Quantum Computing and AI Applications in Industry 5.0 Use Cases. Quantum Computing and Artificial Intelligence: The Industry Use Cases, 435–464.

Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider (J. McAlaney, L. A. Frumkin, & V. Benson, Eds.; pp. 46–63). IGI Global. http://doi.org/10.4018/978-1-5225-4053-3.ch003

Henshel, D., Sample, C., Cains, M., & Hoffman, B. (2016). Integrating Cultural Factors into Human Factors Framework and Ontology for Cyber Attackers. In D. Nicholson (Ed.), Advances in Human Factors in Cybersecurity (Vol. 501, pp. 123–137). Springer International Publishing. https://doi.org/10.1007/978-3-319-41932-9_11

IBM Security. (2023). "Cost of a Data Breach Report 2023". https://www.ibm.com/reports/data-breach

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), 338–345. https://doi.org/10.1109/CIC48465.2019.00047

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. Computers & Security, 70, 663–674. https://doi.org/10.1016/j.cose.2017.08.001

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. Journal of Enterprise Information Management, 34(6), 1597–1629. https://doi.org/10.1108/JEIM-06-2020-0240

Kute, S. S., Tyagi, A. K., & Aswathy, S. U. (2022). Security, Privacy and Trust Issues in Internet of Things and Machine Learning Based e-Healthcare. In A. K. Tyagi, A. Abraham, & A. Kaklauskas (Eds.), Intelligent Interactive Multimedia Systems for e-Healthcare Applications (pp. 291–317). Springer. https://doi.org/10.1007/978-981-16-6542-4_15

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social Engineering: The Neglected Human Factor for Information Security Management. Inf. Resour. Manage. J., 24(3), 1–8. https://doi.org/10.4018/irmj.2011070101

Mahmood, K. (2024). Tech Trends 2024: Emerging Technologies Fueling Digital Transformation. Journal of Emerging Technology and Digital Transformation, 3(01), 45–61.

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. Computers & Security, 95, 101846. https://doi.org/10.1016/j.cose.2020.101846

Mark Elsner, Grace Atkinson, & Saadia Zahidi. (2025). Global Risks Report 2025. World Economic Forum. https://www.weforum.org/publications/global-risks-report-2025/

Milojevic, D., & Nisevic, M. (2024). Navigating cybersecurity challenges in healthcare: Challenges, innovations, and EU legal framework for connected medical devices. In Proceedings of the International Conference on Wearables in Healthcare (pp. 159–181). Springer Nature Switzerland.

Morgan, P. L., Asquith, P. M., Bishop, L. M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020). A New Hope: Human-Centric Cybersecurity Research Embedded Within Organizations. In A. Moallem (Ed.), HCI for Cybersecurity, Privacy and Trust (Vol. 12210, pp. 206–216). Springer International Publishing. https://doi.org/10.1007/978-3-030-50309-3_14

Neupane, A., Saxena, N., Maximo, J. O., & Kana, R. (2016). Neural Markers of Cybersecurity: An fMRI Study of Phishing and Malware Warnings. IEEE Transactions on Information Forensics and Security, 11(9), 1970–1983. https://doi.org/10.1109/TIFS.2016.2566265

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. HOLISTICA – Journal of Business and Public Administration, 9(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review. The 12th International Conference on Advances in Information Technology, 1–11. https://doi.org/10.1145/3468784.3468789

Robinson, N. (2023). Human factors security engineering: The future of cybersecurity teams. EDPACS, 67(5), 1–17.

Rohan, R., Papasratorn, B., Chutimaskul, W., Hautamäki, J., Funilkul, S., & Pal, D. (2023). Enhancing Cybersecurity Resilience: A Comprehensive Analysis of Human Factors and Security Practices Aligned with the NIST Cybersecurity Framework. Proceedings of the 13th International Conference on Advances in Information Technology, 1–16. https://doi.org/10.1145/3628454.3629472

Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S., & Aji, R. F. (2022). Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors. Healthcare, 10(12), 2531. https://doi.org/10.3390/healthcare10122531

THALES. 2024. Data Threat Report: Navigating New Threats and Overcoming Old Challenges. Available at: 2024 Data Threat Report - Navigating New Cybersecurity Threats.

Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. Health Policy and Technology, 10(3), 100549.

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. Journal of Cybersecurity and Privacy, 2(3), Article 3. https://doi.org/10.3390/jcp2030029

Veale, M., & Brown, I. (2020). Cybersecurity. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1533
Verzion Business. (2024). Data Breach Investigations Report.
Verzion Business. (2025). Data Breach Investigations Report.
World Economic Forum (WEF). 2025. "The Global Risks Report 2025". Available at: https://www.weforum.org/publications/global-risks-report-2025/
Yeng, P. K., Yang, B., & Snekkenes, E. A. (2019). Healthcare Staffs' Information Security Practices Towards Mitigating Data Breaches: A Literature Survey. Studies in Health Technology and Informatics, 261, 239–245.
Zhang, R., Xue, R., & Liu, L. (2022). Security and Privacy for Healthcare Blockchains. IEEE Transactions on Services Computing, 15(6), 3668–3686.