Human Factors in Cybersecurity, Vol. 208, 2026, 130–140
https://doi.org/10.54941/ahfe1007419

The Human Factor in Cyber Resilience: Behavioural, Organisational and Sociotechnical Perspectives

Lena von Damaros

Technical Universitiy of Berlin, Institute of Machine Tools and Factory Management, Pascalstraße 8-9, 10587 Berlin, Germany

ABSTRACT

Organisations increasingly recognise that cyber resilience cannot be achieved through technical controls alone, but critically depends on how individuals perceive and enact security requirements in everyday work. This paper synthesises current knowledge on the human factor in cyber resilience at the intersection of behaviour, organisational culture and sociotechnical design. First, core constructs are clarified by linking cyber resilience with established approaches from human factors and work and organisational psychology, including stress and cognitive load, trust and the psychological contract, security culture and human–technology interaction. On this basis, three levels of analysis are distinguished: an individual level (psychological resources and decision processes), an organisational level (leadership, culture, work organisation, perceived fairness and support) and a sociotechnical level (design of technologies, interfaces and digital assistance systems). Second, the paper conducts a structured narrative review of recent empirical and conceptual literature, drawing on seven scientific databases and restricted to peer-reviewed publications from 2023 onwards, to synthesise recurring psychological and organisational mechanisms that influence security-relevant behaviour. Particular attention is paid to tensions between productivity pressures and security demands, as well as to the roles of emotions, fatigue and habituation in real-world decision making. Third, the contribution formulates a literature-based research agenda that highlights key priorities for future interdisciplinary research and for the development of resilience-oriented awareness programmes, leadership practices, work organisation and adaptive sociotechnical solutions.

Keywords: Cyber resilience, Cybersecurity, Human behaviour, Organisational culture, Sociotechnical systems

INTRODUCTION

The digital transformation of modern organisations has fundamentally altered the threat landscape. Cyber incidents are no longer exceptional events but increasingly routine disruptions that organisations must anticipate, absorb, and recover from. While technical safeguards such as firewalls, intrusion detection systems, and encryption remain indispensable, there is growing recognition that technology alone cannot ensure cyber resilience (Ansari et al., 2024; Grobler et al., 2021). The European Union Agency for Cybersecurity (ENISA) and national agencies such as the German Federal

Received May 31, 2026; Revised June 17, 2026; Accepted June 23, 2026; Available online July 20, 2026

Office for Information Security (BSI) consistently report that human behaviour — through errors, omissions, and deliberate actions — is implicated in the majority of cyber incidents (BSI, 2024). This empirical reality underscores the need to move beyond purely technical framings of cybersecurity towards a more comprehensive understanding of the human and organisational dimensions of resilience.

Research consistently identifies human behaviour as both a primary vulnerability and an underutilised resource in organisational cybersecurity. Phishing attacks exploit cognitive biases and emotional reactions; security fatigue leads employees to bypass controls; and inadequate training leaves staff unprepared to respond under pressure (Singh & Cheema, 2024; Kim & Kim, 2024; Bergh & Dupuis, 2025). At the same time, a growing body of evidence suggests that employees who are well-supported, appropriately trained, and embedded in a positive security culture can function as a first line of defence against sophisticated threats (Feraru & Bacali, 2024; Zimmermann et al., 2024). This dual role, simultaneously vulnerability and resource, positions the human factor as a critical lever for organisational cyber resilience that deserves sustained scholarly attention.

Despite this recognition, the psychological and organisational dimensions of cyber resilience remain fragmented across disciplines, with research addressing individual factors in isolation and technical perspectives dominating the literature (Khadka & Ullah, 2025; Pollini et al., 2021). This paper addresses this gap through a structured narrative review that synthesises psychological, organisational, and sociotechnical mechanisms across three analytical levels (individual, organisational, and sociotechnical) and formulates a literature-based research agenda with practical implications for resilience-oriented programmes and work design.

THEORETICAL BACKGROUND

Cyber Resilience: Definition and Scope

Cyber resilience is understood as the ability of an organisation to anticipate, withstand, recover from, and continuously adapt to adverse cyber events (Ansari et al., 2024). This concept extends traditional cybersecurity, which focuses primarily on the prevention of unauthorised access, by incorporating preparedness, response, and learning as equally important dimensions. Unlike a purely technical framing, cyber resilience acknowledges that disruptions are inevitable and that organisational capacity to absorb and learn from incidents is as critical as the ability to prevent them (Aakassh et al., 2024).

The Human Factor: Conceptual Clarification

The term ‘human factor’ encompasses individual phenomena (cognitive processes, stress, fatigue, emotional arousal) and collective phenomena (shared norms, values, security culture) that influence security-relevant behaviour (Singh & Cheema, 2024; Feraru & Bacali, 2024). Drawing on engineering, work psychology, and behavioural economics, it provides an interdisciplinary lens on why individuals and organisations behave as they do in the face of cyber risk (Thron et al., 2024).

Relevant Theoretical Frameworks

Three theoretical frameworks structure the analysis. Cognitive Load Theory (Sweller, 1988) explains how depleted cognitive resources increase errors and non-compliance under workload or time pressure (Kim & Kim, 2024). The Psychological Contract (Rousseau, 1989) links perceived organisational fairness and support to intrinsic security motivation: contract breach reduces voluntary compliance (Kim & Kim, 2024; Isik et al., 2024). Sociotechnical Systems Theory (Trist & Bamforth, 1951) holds that technical and social subsystems must be jointly optimised: interface design and system architecture cannot be assessed independently from the human, organisational, and cultural contexts in which they operate (Thron et al., 2024; Aakassh et al., 2024).

METHODOLOGY

This paper employs a structured narrative review to synthesise current knowledge on the human factor in cyber resilience. The approach combines a transparent, documented literature search with thematic, interpretive synthesis, making it well-suited for interdisciplinary topics where the goal is conceptual insight rather than statistical aggregation of results (Sukhera, 2022; Green et al., 2006). Retained literature was read in full, coded thematically, and synthesised across sources to identify recurring mechanisms, empirical patterns, and open questions. The search strategy and inclusion criteria are summarised in Table 1.

Table 1: Search strategy and inclusion criteria.

Criterion	Details
Databases	IEEE Xplore, ACM Digital Library, Semantic Scholar, ScienceDirect, SpringerLink, Web of Science, Scopus
Search strings	(“human factor” OR “human behaviour”) AND (“cyber resilience” OR “cybersecurity”) AND (“organisational culture” OR “sociotechnical” OR “security behaviour” OR “psychological contract” OR “cognitive bias” OR “security fatigue”)
Publication period	2024–2026
Document types	Peer-reviewed journal articles; conference papers
Thematic focus	Substantive engagement with human, psychological, or organisational dimensions of cybersecurity or cyber resilience
Exclusion criterion	Studies focusing exclusively on technical security mechanisms without human or organisational reference
Final corpus	18 sources (empirical studies, conceptual papers, structured reviews)

Synthesis Approach

Retained articles were coded thematically according to three analytical levels derived from the review framework: individual psychological factors, organisational factors, and sociotechnical factors. Within each level, recurring mechanisms and empirical findings were identified and synthesised into

thematic clusters. The synthesis proceeds narratively, integrating findings across sources to identify patterns, convergences, and areas of remaining uncertainty. A structured evidence table (Table 2) documents the key studies reviewed, their thematic focus, and main findings, providing a transparent basis for the synthesis presented in Section 4.

REVIEW FINDINGS: PSYCHOLOGICAL AND ORGANISATIONAL MECHANISMS

The structured narrative review identified three analytically distinct yet interrelated clusters of mechanisms through which human factors shape cyber resilience: psychological factors at the individual level, organisational factors at the collective level, and sociotechnical factors at the interface between people and technology. The following subsections synthesise empirical and conceptual findings within each cluster.

Individual-Level Psychological Factors

At the individual level, stress and cognitive load impair security decision-making, increasing susceptibility to social engineering and heuristic-driven errors (Singh & Cheema, 2024; Kim & Kim, 2024; Bergh & Dupuis, 2025). Overexposure to security demands generates cybersecurity fatigue, a motivational depletion state that fosters habitual non-compliance, (Sangwan, 2024; Kim & Kim, 2024). Cognitive biases (authority, urgency, status quo) are systematically exploited by attackers, while emotional responses to incidents can both motivate and impair protective behaviour (Tsanov, 2024; Fatima et al., 2024).

Organisational-Level Factors

Organisational culture is among the most robust predictors of security behaviour: psychological safety cultures foster compliance, proactive reporting, and collective resilience, while blame-centric cultures suppress the incident reporting necessary for improvement (Isik et al., 2024; Patterson et al., 2024). The psychological contract shapes intrinsic security motivation: perceived unfairness and inadequate support reduce voluntary compliance substantially (Kim & Kim, 2024; Feraru & Bacali, 2024). Transformational leadership fosters security culture maturity, while tailored training programmes that address fatigue and social influence outperform generic compliance-oriented formats (Friday et al., 2024; Colabianchi et al., 2025).

Sociotechnical Factors

At the sociotechnical level, poorly designed security systems, generating alert fatigue, excessive friction, or cognitive overload, undermine compliance by making secure behaviour more burdensome than insecure alternatives (Zimmermann et al., 2024; Khadka & Ullah, 2025). Nudging interventions (visual cues, timely reminders, real-time feedback) improve behaviour with low cognitive cost, and ethnographic evidence from SMEs confirms that effective design must accommodate workable adjustments rather

than prescribe ideal solutions (Kocksch & Jensen, 2024). Automation bias (over-reliance on technical safeguards) creates invisible gaps that effective sociotechnical design must address by maintaining appropriate human engagement (Tsanov, 2024; Zimmermann et al., 2024).

Table 2 summarises the studies included in the review. The "Construct" column indicates the primary theoretical concept or variable each study examines (e.g. security behaviour, organisational culture, or cyber resilience capability); "Key Finding" presents the study's central empirical result relevant to the human factor in cyber resilience.

Table 2: Key empirical studies reviewed (2024–2026). *Level: I = Individual, O = Organisational, ST = Sociotechnical.

Author(s) & Year	Construct	Level*	Key Finding
Singh & Cheema (2024)	Stress, cognitive biases	I	Stress impairs decision quality; cognitive biases (authority, urgency) increase susceptibility to social engineering.
Kim & Kim (2024)	Burnout, fatigue, psych. contract	I	Burnout mediates non-compliance; psychological contract breach reduces intrinsic security motivation.
Bergh & Dupuis (2025)	Stress & phishing	I	Experimentally induced stress significantly reduces phishing detection accuracy.
Tsanov (2024)	Cognitive biases, SE tactics	I	Authority and urgency biases are systematically exploited; habituation leads to ignored warnings and risky repetition.
Sangwan (2024)	Cybersecurity fatigue	I	Overexposure to security demands produces motivational depletion; beyond a threshold, frequency breeds disengagement.
Virtanen (2024)	Psych. strain, situational awareness	I	Psychological strain during cyber incidents impairs situational awareness and structured incident response; feelings of guilt and purpose coexist, with leadership and clear roles as key mitigating factors.
Fatima et al. (2024)	Emotional resilience, communication	I / O	Emotional resilience and clear management communication sustain performance during cyber incidents.
Friday et al. (2024)	Awareness training (SMEs)	O	Tailored SME training reduces incidents 45–65%; management commitment and contextual relevance are essential.
Isik et al. (2024)	Psych. safety, blame culture	O	Blame cultures suppress reporting; just culture approaches enable collective learning and resilience.
Patterson et al. (2024)	Org. learning from incidents	O	Cultural openness enables learning from incidents; defensiveness and blame attribution systematically hinder improvement.
Feraru & Bacali (2024)	Intrinsic motivation, leadership	O	Transformational leadership fosters internalisation of security norms as genuine values (SDT).
Avrahami & Zwilling (2025)	CTI, employee behaviour	O	Structured CTI programmes improve threat identification and adaptive security behaviour across staff levels.

(Continued)

Table 2: Continued.

Author(s) & Year	Construct	Level*	Key Finding
Mahmood et al. (2024)	STS, crisis conditions	O / ST	Crisis conditions amplify human vulnerabilities; resilience requires aligned optimisation of people, technology, and processes.
Gerst et al. (2024)	Security culture (SMEs)	O	SME security culture depends on leadership commitment, dedicated resources, and contextually relevant awareness initiatives.
Zimmermann et al. (2024)	Human-centred design	ST	Enabling design (friction reduction, workflow alignment) outperforms purely constraining approaches.
Kocksch & Jensen (2024)	Sociotechnical practice (SMEs)	ST	Security in practice is adaptive and improvisational; design must accommodate real constraints, not prescribe ideal solutions.
Nganga et al. (2024)	HF in maritime cyber resilience	ST	High workload and culture shape human–system interaction; workload degrades resilience by increasing error rates.
Khadka & Ullah (2025)	Psych. resilience, ST integration	I / ST	Four pillars: psychological resilience, adaptive learning, emotional intelligence, and sociotechnical integration.
Colabianchi et al. (2025)	HF as strategic opportunity	O / ST	Reframing human factors as strategic opportunity yields stronger security posture and adaptive resilience.

KEY TENSIONS AND CHALLENGES

The review findings reveal several persistent tensions that reflect deep structural conflicts between competing organisational priorities, cognitive limitations, and everyday work realities.

Productivity Pressure versus Security Requirements

One of the most consistently reported tensions in the literature is the conflict between productivity demands and security requirements. Security measures that generate friction (mandatory multi-factor authentication, strict access controls, frequent password changes, or lengthy verification procedures) are routinely perceived by employees as obstacles to efficient work completion (Kocksch & Jensen, 2024; Isik et al., 2024). Under time pressure, employees systematically prioritise task completion over security compliance, making workarounds and shortcut behaviours rational responses to an organisational environment that implicitly rewards speed over caution (Friday et al., 2024; Bergh & Dupuis, 2025). This tension cannot be resolved through awareness training alone; it requires structural interventions that redesign work processes and security mechanisms to reduce the friction cost of secure behaviour.

Cybersecurity Fatigue and Habituation

Repeated security demands generate cybersecurity fatigue: a motivational depletion state that undermines compliance and, beyond a threshold, breeds disengagement rather than vigilance (Kim & Kim, 2024; Mızrak et al., 2025).

Closely related, habituation normalises risk: employees learn to ignore warnings without consequences, and routine phishing simulations may build test-format awareness without genuine behavioural change (Tsanov, 2024; Khan et al., 2025).

Over-reliance on Technology

A third tension concerns the relationship between technical safeguards and human agency. As organisations deploy increasingly sophisticated automated security tools (endpoint detection, AI-driven threat monitoring, automated incident response), employees may develop a false sense of security that reduces their personal security vigilance (Tsanov, 2024; Akre et al., 2025). This automation bias is particularly problematic because it creates invisible gaps: employees assume the system will catch errors they make, while the system is designed around the assumption that humans will provide a complementary layer of vigilance. Zimmermann et al. (2024) argue that this dynamic can only be addressed by redesigning the human-technology relationship: moving from a model where technology compensates for human failure towards one where humans and technology collaborate as genuine partners, each informed by the other's capabilities and limitations.

Knowledge-Practice Gap

A fourth challenge, documented across multiple organisational contexts, is the gap between security knowledge and actual behaviour. Employees who can correctly identify phishing emails in training scenarios may still click on suspicious links under real-world time pressure; those who understand password hygiene may still reuse credentials for convenience (Hore et al., 2024; Malik & Malik, 2025). This knowledge-practice gap reflects the primacy of situational and contextual factors over declarative knowledge in shaping behaviour. It calls for training approaches that simulate realistic conditions, embed secure habits in the flow of daily work, and address the emotional and motivational (not merely cognitive) dimensions of security behaviour.

RESEARCH AGENDA AND IMPLICATIONS

The fragmentation of psychological, organisational, and sociotechnical perspectives identified in this review points to a core gap: the absence of integrated, multilevel approaches capable of capturing how individual behaviour, organisational culture, and system design interact in shaping cyber resilience. The following priorities address this gap directly.

Priorities for Interdisciplinary Research

Most urgently, the field needs longitudinal, multilevel study designs that simultaneously track individual psychological states, team norms, and cultural factors over time, moving beyond the cross-sectional, single-factor studies that currently dominate (Patterson et al., 2024; Kim & Kim, 2024). Such designs would allow researchers to model how fatigue accumulates, how culture develops after incidents, and how resilience is sustained or eroded: these

are questions that existing research cannot adequately answer. In parallel, sociotechnical design research should evaluate under which conditions secure behaviour becomes the default, assessing nudging, adaptive interfaces, and AI-assisted decision support not only for immediate effectiveness but for long-term user acceptance (Khan et al., 2025; Zimmermann et al., 2024). Finally, SME-specific studies are overdue: the organisational realities of flat hierarchies, limited specialisation, and dual operational-security roles create conditions that large-organisation findings cannot adequately model (Kocksch & Jensen, 2024; Gerst et al., 2024).

Implications for Practice

Training programmes should shift from compliance-oriented knowledge transmission towards behaviour-centred, contextually embedded approaches that address fatigue, social influence, and emotional responses to threat (Friday et al., 2024; Colabianchi et al., 2025). Gamification, realistic simulation, and timely positive feedback sustain engagement more effectively than one-off mandatory training.

Leadership should cultivate psychological safety and a 'just culture' that distinguishes systemic failures from individual negligence, treating incidents as learning opportunities (Isik et al., 2024; Patterson et al., 2024). Visible leadership commitment to security values remains one of the most powerful driver of organisational security culture.

Work design should treat cognitive load, fatigue, and time pressure as structural risk factors: scheduling high-stakes tasks at low-demand periods, providing recovery time for security operations staff, and filtering alert volumes intelligently (Akre et al., 2025; Sobulo, 2025). Sociotechnical interventions (interface redesign, default-secure configurations, AI-assisted decision support) should be co-designed with end users to align tools with real workflows (Kocksch & Jensen, 2024; Khan et al., 2025).

CONCLUSION

This paper has conducted a structured narrative review of recent empirical and conceptual literature to synthesise the mechanisms through which human factors shape organisational cyber resilience.

Across three analytical levels, the review identifies stress, fatigue, cognitive biases, and emotional arousal as individual determinants; security culture, leadership, and the psychological contract as organisational drivers; and interface design, nudging, and automation bias as sociotechnical factors shaping secure behaviour. Organisations that invest in psychological safety and a just culture demonstrate stronger resilience, while human-centred design positions technology as an enabler rather than a replacement for human judgment.

Three major tensions cut across these levels: the conflict between productivity pressure and security demands, the problem of cybersecurity fatigue and habituation, and the risk of over-reliance on automated technical controls. Addressing these tensions requires integrated interventions that simultaneously target individual motivation, organisational culture, and

system design, treating employees not as the 'weakest link' to be controlled, but as a critical resource to be supported, developed, and engaged.

Four research priorities emerge. First, longitudinal designs are needed to track how fatigue accumulates, how security culture evolves after incidents, and how resilience is sustained or eroded over time. Second, multilevel empirical studies should simultaneously examine individual, organisational, and sociotechnical factors to capture the interactions between levels that single-focus studies cannot address. Third, sociotechnical intervention research should evaluate nudging, adaptive interfaces, and AI-assisted decision support not only for short-term effectiveness but for long-term behavioural transfer and user acceptance. Fourth, SME-specific studies are overdue, as the distinct organisational conditions of small and medium-sized enterprises (including flat hierarchies, limited resources, and dual operational-security roles) cannot be adequately captured by findings from large organisations. Collectively, these priorities reflect the need for an interdisciplinary science of human-centred cyber resilience that matches the complexity and urgency of the challenge.

REFERENCES

Akre, V., Kobbaey, T., Lazarov, G., Abdulsalam, K., Al-Sit, W., & Diab, J. (2025). From alert fatigue to augmented defense: A case for AI copilots in cybersecurity operation centers. Proceedings of the IEEE International Conference on Intelligent Technologies and Telecommunications (ITT). https://doi.org/10.1109/ITT69610.2025.11352895

Ansari, I. S., Asghar, M. R., & AlHidaifi, S. M. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. ACM Computing Surveys, 56(8), Article 196. https://doi.org/10.1145/3649218

Avrahami, Z., & Zwilling, M. (2025). The impact of cyber threat intelligence (CTI) on employee behavior and skills and the implications for organizational cyber resilience. International Journal of Information Security. Advance online publication. https://doi.org/10.1007/s10207-025-01096-y

Bergh, C., & Dupuis, M. J. (2025). Cybersecurity is stressful: The impact of stress on identifying phishing attacks. In Proceedings of the 5th IEEE Cyber Awareness and Research Symposium (CARS 2025). https://doi.org/10.1109/CARS67163.2025.11337636

BSI (2024). Lagebericht zur IT-Sicherheit in Deutschland 2024. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

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). https://doi.org/10.1016/j.jik.2025.100695

Fatima, F., Hyatt, J. C., Rehman, S. U., De La Cruz, E., Nadella, G. S., & Meduri, K. (2024). Resilience and risk management in cybersecurity: Emotional, psychological, and organizational dynamics. Journal of Economy and Technology, 2, 247–257. https://doi.org/10.1016/j.ject.2024.08.004

Feraru, I., & Bacali, L. (2024). Explore the intersection of self-determination theory and cybersecurity education: A literature review. International Journal of Advanced Studies in Information Technology and e-Learning Systems, 2(1). https://doi.org/10.2478/ijasitels-2024-0017

Friday, U., Aina, O., Abass, M., & Kushanu, D. (2024). Employee cybersecurity awareness training programs customized for SME contexts. Journal of Knowledge and Learning Science Technology, 3(3). https://doi.org/10.60087/jklst.vol3.n3.p382-409

Gerst, M., Kappe, M., Härting, R.-C., & Karg, C. (2024). Determinants of the successful establishment of a cyber security culture in SMEs. Procedia Computer Science, 246, 510–518. https://doi.org/10.1016/j.procs.2024.09.431

Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: Secrets of the trade. Journal of Chiropractic Medicine, 5(3), 101–117.

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. Frontiers in Big Data, 4, 583723. https://doi.org/10.3389/fdata.2021.583723

Hore, K., Tan, M. H., & Magner, C. (2024). Cybersecurity and critical care staff: A mixed methods study. International Journal of Medical Informatics, 186, 105412. https://doi.org/10.1016/j.ijmedinf.2024.105412

Isik, Ö., Viskovich, Y., & Pavitt, S. (2024). Common pitfalls when mitigating cyber risk: Addressing socio-behavioural factors. IMD Business School Working Paper. https://doi.org/10.69554/ueev5385

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. International Journal of Information Security, 24(3). https://doi.org/10.1007/s10207-025-01032-0

Khan, N., Sharples, S., & Houghton, R. (2025). Reflective interventions for cybersecurity: Insights from a sociotechnical framework application and assessment. Cognition, Technology & Work. Advance online publication. https://doi.org/10.1007/s10111-025-00833-6

Kim, B.-J., & Kim, M.-J. (2024). The influence of work overload on cybersecurity behavior: A moderated mediation model of psychological contract breach, burnout, and self-efficacy. Technology in Society, 77, 102543. https://doi.org/10.1016/j.techsoc.2024.102543

Kocksch, L., & Jensen, T. E. (2024). The mundane art of cybersecurity: Living with insecure IT in Danish small- and medium-sized enterprises. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW2). https://doi.org/10.1145/3686893

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Addressing cybersecurity challenges in times of crisis: Extending the sociotechnical systems perspective. Applied Sciences, 14(24), 11610. https://doi.org/10.3390/app142411610

Malik, I., & Malik, A. (2025). Decision fatigue and cybersecurity behaviors: A qualitative study of university students. Journal of Information Systems Engineering & Management, 10(58s). https://doi.org/10.52783/jisem.v10i58s.12613

Mızrak, F., Demirel, H. G., Yaşar, O., & Karakaya, T. (2025). Digital detox: Exploring the impact of cybersecurity fatigue on employee productivity and mental health. Discover Mental Health, 5, 35. https://doi.org/10.1007/s44192-025-00149-x

Nganga, A., Scanlan, J., Lützhöft, M., & Mallam, S. (2024). Enabling cyber resilient shipping through maritime security operation center adoption: A human factors perspective. Applied Ergonomics, 119, 104312. https://doi.org/10.1016/j.apergo.2024.104312

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2024). 'I don't think we're there yet': The practices and challenges of organisational learning from cyber security incidents. Computers & Security, 139, 103699. https://doi.org/10.1016/j.cose.2023.103699

Pollini, A., Callari, T., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Technology & Work, 24, 375–398. https://doi.org/10.1007/s10111-021-00683-y

Sangwan, A. (2024). Human factors in cybersecurity awareness. 2024 International Conference on Intelligent Systems for Cybersecurity. https://doi.org/10.1109/ISCS61804.2024.10581139

Singh, B., & Cheema, S. S. (2024). Psychology in cybersecurity: Unveiling the human dimensions of digital resilience. International Journal of Advanced Networking and Applications, 16(1), 6281–6290. https://doi.org/10.35444/ijana.2024.16107

Sobulo, S. A. (2025). Human limits in cyber defence: Sleep, stress, and security risk. International Journal of Multidisciplinary Research and Growth Evaluation, 6(6). https://doi.org/10.54660/.ijmrge.2025.6.6.1229-1231

Sukhera, J. (2022). Narrative reviews: Flexible, rigorous, and practical. Journal of Graduate Medical Education, 14(4), 414–417. https://doi.org/10.4300/jgme-d-22-00480.1

Thron, E., Faily, S., Dogan, H., & Freer, M. (2024). Human factors and cybersecurity risks on the railway: The critical role played by signalling operations. Information and Computer Security, 32(2), 236–263. https://doi.org/10.1108/ics-05-2023-0078

Tsanov, V. (2024). Social engineering and cognitive biases in cybersecurity. Proceedings of the International Conference on Automatics and Informatics (ICAI 2024). https://doi.org/10.1109/ICAI63388.2024.10851536

Virtanen, T. (2024). Psychological effects of continuity threatening cyber incidents. Proceedings of the 23rd European Conference on Cyber Warfare and Security (ECCWS), 23(1). https://doi.org/10.34190/eccws.23.1.2268

Zimmermann, V., Nitsch, M., Kolb, J., & Peisl, T. (2024). Human-centered cybersecurity revisited: From enemies to partners. Communications of the ACM, 67(6), 56–63. https://dl.acm.org/doi/10.1145/3665665