*Human Factors in Cybersecurity,* Vol. 208, 2026, 11–20
https://doi.org/10.54941/ahfe1007408

# Cognitive Load and Compliance: A Human-Centric Framework for NIS2 in Latvian SMEs

**Imants Breidaks[1], Henrijs Kalkis[1,2], and Anton Semenov[3]**

[1]University of Latvia, Faculty of Medicine and Life Sciences, Riga, Latvia
[2]University of Latvia, Faculty of Business, Management and Economics, Riga, Latvia
[3]Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

## ABSTRACT

The transposition of the EU NIS2 Directive into Latvia's National Cybersecurity Law (NKDL) significantly expands the scope of regulation: from ~1,000 to ~8,000 organizations, many of them SMEs without dedicated security teams. The aim of this paper is to develop a human-centric compliance framework for Latvian SMEs that operationalizes selected NIS2/NKDL cybersecurity requirements through a cognitive-load perspective. This paper frames NIS2 compliance as a cognitive ergonomics problem and develops a low-friction "NIS2 Compliance Starter Pack" that reduces response cost while preserving auditable evidence. Using a socio-technical synthesis, NKDL obligations are mapped to pragmatic controls and to workload indicators derived from the NASA Task Load Index (NASA-TLX). The developed framework prioritizes secur-by-default interventions - such as default multifactor authentication, automated security nudges, and micro-learning - over high-intensity training that often produces fatigue and workarounds. Sustainable cyber resilience is treated as an engineered property of the work system rather than a checklist outcome.

**Keywords:** NIS2 directive, Human factors, Cognitive load, SMEs, Cybersecurity, NASA-TLX

## INTRODUCTION

Directive (EU) 2022/2555 (NIS2) raises the baseline expectations for cybersecurity risk management and governance across a wider set of sectors than the previous NIS framework (European Union, 2022). It requires in-scope organizations to implement a range of measures, such as risk analysis, incident handling, business continuity planning, and supply-chain security, and ensures executive accountability for cybersecurity. For Latvia, this is codified through the National Cybersecurity Law (NKDL) and Cabinet Regulation No. 397, which specify baseline cybersecurity requirements for supervised entities (Cabinet of Ministers of the Republic of Latvia, 2025; Saeima of the Republic of Latvia, 2024). These instruments vastly expand the number of organizations under supervision, bringing many resource-constrained entities into the compliance fold (Saeima of the Republic of Latvia, 2024). A significant portion of the newly in-scope organizations are small and medium-sized enterprises (SMEs) that lack dedicated security teams or Security Operations Centers (SOCs). This context creates a

Received February 28, 2026; Revised March 30, 2026; Accepted April 16, 2026; Available online July 20, 2026

practical challenge: how can SMEs meet strict cybersecurity obligations without incurring excessive cognitive and operational burdens on their staff? And it is evident that the overall complexity of cybersecurity (and security in general) is rising across diverse fields. For example, in the energy sector, recent reviews of cyber-physical systems (such as smart grids) emphasize that increased connectivity expands the attack surface and raises the operational stakes of cyber incidents (Alomari et al., 2025).

Human factors research suggests that compliance failures often arise not from lack of awareness or carelessness, but from misaligned system design and cognitive overload (Khadka and Ullah, 2025; Nobles, 2022). Nobles and Robinson (2024) describe Human Factors Engineering (HFE) as the "missing discipline" in cybersecurity, arguing that many security policies overestimate human capacities and lead to "security fatigue" - a state of exhaustion and resignation in the face of constant security demands. Indeed, evidence shows the human element remains a major factor in breaches: the 2025 Verizon DBIR reports that roughly 60% of breaches involve a human component (Verizon, 2025). Attackers continue to exploit social engineering and other human-centric attack vectors, as highlighted in ENISA's Threat Landscape 2025 report (ENISA, 2025b). Recent quantitative work likewise treats social engineering prevention as a combined behavioral and technical challenge (Tan et al., 2025). In response, regulators and agencies have begun to emphasize the human element. ENISA, for example, has issued guidance mapping NIS2 obligations to roles and skills (ENISA, 2025a) and conducted studies on cybersecurity investment needs (ENISA, 2025c), signaling that compliance is evolving into an ongoing organizational capability rather than a one-off checklist. This broader context underscores the need to approach NIS2 compliance not just as a legal exercise, but as a work-system design problem (Nobles and Robinson, 2024).

A publicly available Latvian SME survey ($n \approx 900$) was used to identify common gaps in training, budgeting, and continuity planning (Tet, 2022). This 2022 survey found that many SMEs perceived cyber risks, at least at the time of the survey, as a low priority, leading to minimal investments and ad hoc security measures. This baseline was used (while recognizing it as self-reported) to ground understanding of typical SME readiness.

The aim of this paper is to develop an ergonomic framework for engineering NIS2 compliance in Latvian SMEs that reduces cognitive load and response cost while producing evidence artefacts suitable for regulatory oversight. The framework operationalizes selected NIS2 requirements as low-friction, auditable work practices. It adopts a socio-technical perspective and treats compliance as an outcome of ergonomic system design: when controls exceed the cognitive capacity of non-specialists, workarounds and fatigue become rational adaptations. This framing aligns with recent work on the psychology of cybersecurity, which highlights the role of workload and everyday constraints in security behavior (Hadlington and Ryding, 2026).

## CONCEPTUAL BACKGROUND

Two concepts from human factors and behavioral security are key to this approach: response cost and work-system fit. *Response cost* refers to the

perceived effort, time, or other inconvenience associated with a protective action. In the protection-motivation theory, high perceived response costs reduce the likelihood that even well-intentioned individuals will conduct security behaviors under pressure (Kiran et al., 2025). In other words, if a security measure makes a task significantly slower or harder, practitioners may rationally choose to bypass it to meet immediate work goals. *Work-system fit* refers to how well security controls integrate with the user's actual workflow and constraints. When a control conflicts with operational realities - such as production deadlines, safety procedures, or usability norms - users often develop workarounds to get the job done (Nobles and Robinson, 2024). This phenomenon is widely observed: for example, requiring complex logins on shared devices or mandating lengthy incident forms during critical operations can lead staff to create unofficial shortcuts. Secure behavior should be treated as an engineered property of the system, not simply a matter of awareness or discipline (Nobles, 2022). Designing for low response cost and high work-system fit means building security measures that are as invisible and low-effort as possible for end-users, so that the path of least resistance is also the secure path.

## MATERIALS AND METHODS

This study uses a targeted scoping synthesis to translate NIS2's high-level requirements into an operational, cognitive-fit framework. Approximately 250 sources were screened; forty peer-reviewed and policy documents were retained for final synthesis. No new empirical data are collected; instead, the paper consolidates insights from recent peer-reviewed literature, secondary data sources, and policy guidance (2022–2026) to inform design principles. The approach involved three steps. First, an indicative SME baseline was derived from publicly available secondary material (Tet, 2022) and treated as contextual input rather than primary evidence. Second, key human-factor stressors and mechanisms were extracted from recent interdisciplinary studies and frameworks on cybersecurity behavior and compliance burden (e.g., Khadka and Ullah, 2025; Desolda et al., 2025). Sources from 2021–2025 were prioritized that specifically address cognitive workload, security behavior, and socio-technical factors. Third, selected NIS2 risk-management requirements were mapped to operations-friendly interventions and evidence artefacts, cross-checked against implementation guidance and security standards (ENISA, 2025d; Boyens et al., 2022; Stouffer et al., 2023). Researchers focused on NIS2 Article 21(2) risk-management measures that seemed most prone to compliance frictions in SME contexts (e.g., security policies, incident handling, continuity planning, supply-chain security, and training). For each, official implementation guidance was consulted, and industry best practices were used to identify interventions that minimize disruption. Table 1 presents an excerpt of this mapping as a Human-Centric Compliance Matrix, linking each control objective to a likely failure mode (if addressed in a purely "paper" manner) and to a practical intervention that aligns with work-as-done.

This assessment was also informed by the authors' practitioner and entrepreneurial experience in SMEoriented cybersecurity services, ergonomics, and essentialservice operations, which served as a plausibility check for the hypothesized failure modes and pragmatic interventions.

During the preparation of this manuscript, the authors utilized AI-based tools (Scopus AI, Gemini, Perplexity, and ChatGPT) to assist in literature discovery and language refinement. All screening decisions, syntheses, and final content were determined by the authors, who take full responsibility for the integrity and accuracy of this publication.

## RESULTS AND DISCUSSION

### Four-Phase Human-Centric Compliance Framework

To operationalize the above concepts, a four-phase framework, "NIS2 Compliance Starter Pack," is proposed (Figure 1) to integrate NIS2 compliance into SME operations with minimal cognitive resistance. The phase sequence follows an ergonomics-based logic: context calibration, workload assessment, intervention design, and evidence-driven feedback, adapted to NIS2 governance and auditability requirements. The phases are:

1. Baseline and Context Analysis. Identify the organization's key assets, workflows, and existing cybersecurity gaps. This includes mapping out the standard tasks employees perform that have security implications (e.g., system logins, remote access, software updates) and assessing current pain points or workaround practices. It also involves understanding regulatory scope (which NIS2 obligations apply) and the business context (e.g., critical processes, resource constraints). The output of the first phase is a tailored compliance baseline that highlights where "paper compliance" (policy-on-paper) is likely misaligned with everyday work.
2. Task Load Assessment. Evaluate the cognitive and operational load imposed by required security tasks. This phase applies the NASA-TLX workload index (or comparable instruments) to rate the dimensions of Mental Demand, Physical Demand, Temporal Demand, Performance, Effort, and Frustration for typical security-related activities (Aksu et al., 2025). By quantifying what workers find most taxing or frustrating, the second phase identifies compliance tasks most likely to fail without redesign. For example, if employees rate routine password updates or incident reporting procedures as high in Temporal Demand and Frustration, these are prime candidates for intervention.
3. Secure-by-Design Interventions. Implement low-friction controls and support tools that embed security into workflows with minimal user effort. Based on insights from the second phase, the organization deploys the proposed "NIS2 Compliance Starter Pack" (a low-cost intervention cluster). It includes measures such as default-on MFA (making multi-factor authentication the path of least resistance), automated security nudges (removing the memory burden), and gamified micro-learning modules, which recent literature associates with lower perceived workload and

improved engagement (Pramod, 2024). These interventions are chosen to reduce specific NASA-TLX workload dimensions. For instance, automating routine checks lowers Temporal Demand, while gamified training decreases Frustration. The goal is to engineer secure behavior by default, making the secure action the easiest (or only) option. All interventions are aligned with NIS2's requirements, but they prioritize human usability: security is built with the operator in mind rather than as an afterthought.

4. Continuous Improvement and Evidence. In this phase, establishing feedback is critical to monitor the effectiveness of controls and adjust as needed. NIS2 obliges entities to provide evidence of the effectiveness of their cybersecurity measures (European Union, 2022), so the fourth phase integrates compliance monitoring with operational metrics. This may involve lightweight data collection such as tracking incident reports (to ensure timely reporting), logging MFA usage rates, or conducting brief post-incident surveys on workload. The idea is to continually validate that the interventions from the third phase are achieving their intended effect (e.g., reducing errors or workarounds) and not inadvertently introducing new burdens. Fourth-phase outputs include both internal learning (e.g., identifying a need for refresher micro-learning when certain mistakes recur) and external compliance evidence (audit-friendly records such as training completion rates, incident response timelines, or system uptime during security events). Over time, this creates an evidence-driven improvement cycle that moves the organization away from static annual checklists toward a dynamic risk management practice. Comparable evidence-driven governance loops that use field-layer telemetry to support NIS2-aligned risk evaluation have been demonstrated in railway infrastructure (Wachnik et al., 2025).

SMEs could iterate through these phases in an agile manner, starting with a single high-priority control (e.g., incident handling) and cycling through phases1-4 for that area.

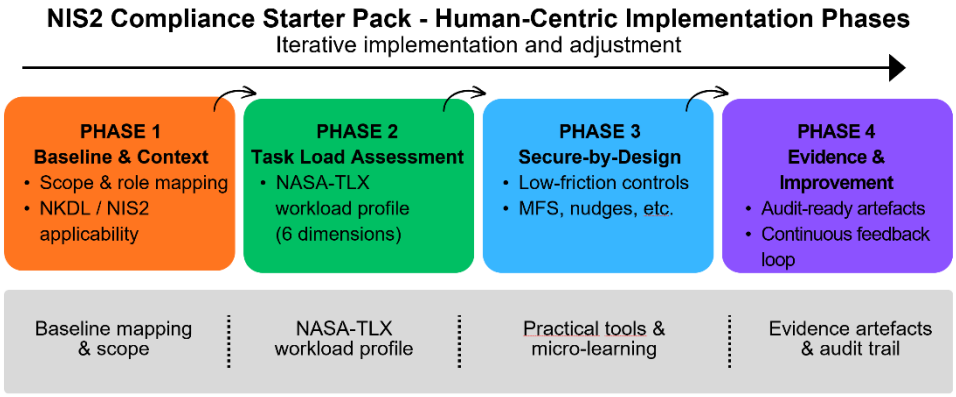


**Figure 1:** The four-phase human-centric compliance framework and its relationship to workload management and evidence generation.

**Table 1:** Human-centric compliance framework for Latvian SMEs: considering NIS2/NKDL cybersecurity requirements through a cognitive-load perspective.

| NIS2 Art. 21(2) Requirement | Failure Mode (Socio-Technical Friction) | Operations-Friendly Intervention | Evidence (Audit Artifacts) |
|---|---|---|---|
| **(a) Risk analysis & info syestem security** | Risk analysis and asset inventory remain confined to IT; Operational Technical (OT) assets or shop-floor workflows are overlooked. | Extend asset inventory and risk assessment to include OT/CPS* assets; connect risk treatment plans to operational procedures and maintenance schedules. | Expanded asset inventory covering OT*; risk register entries linked to SOPs; minutes of periodic risk review meetings. |
| **(b) Incident handling** | Under pressure of time or fear of blame, incidents go unreported, or only IT staff are involved (operations staff bypass formal reporting). | Establish a no-blame incident-reporting policy and channel; conduct OT-inclusive incident-response drills; provide short, role-specific incident runbooks for shift supervisors. | Incident log with timestamps and entries from all roles; drill and tabletop exercise reports; after-action review documents showing issues identified and resolved. |
| **(c) Business continuity & backup management** | Backups exist, but restore procedures are untested for OT configurations; downtime tolerances are not clearly defined, leading to improvised decisions in a crisis. | Schedule regular restore tests for critical OT systems; define a "minimum viable" operating mode for emergencies; align backup/recovery steps with safety protocols. | Records of backup restore tests, documented recovery time and recovery point targets, and a simple recovery checklist. |
| **(d) Supply chain security** | Vendor remote access remains always-on or uses shared credentials; temporary exceptions granted for vendors become permanent. | Enforce time-bound vendor access with mandatory MFA; integrate access approvals with work orders; segregate and monitor vendor sessions on critical systems. | Vendor access logs linked to work orders; MFA logs for vendor accounts; supplier security review reports; register of access exceptions with expiration dates. |
| **(g) Basic cyber hygiene & training** | Generic security training is not relevant to operational roles; frontline operators miss key guidance, and secure practices are not reinforced in daily tasks. | Provide role-based "micro-training" modules (short, focused lessons) and just-in-time job aids for high-risk activities (e.g., checklists for remote connections). | Training completion records segmented by role; micro-learning participation stats; results of knowledge checks; trend analysis of human-factor incidents. |

* OT/CPS - Operational Technology (OT) manages industrial processes, while Cyber-Physical Systems (CPS) bridge computation with physical action.

Note: The failure modes in Table 1 are practitioner-informed hypotheses derived from the literature synthesis; they are not directly measured in this study and require empirical validation.

Several themes emerge from the framework and compliance matrix.

First, evidence-driven compliance is crucial. NIS2 not only asks organizations to implement controls but also to verify their effectiveness (European Union, 2022). Embedding measurements in the fourth phase (e.g., logging incidents, tracking training outcomes) ensures that compliance is not a documentation-focused implementation process but a performance-based activity. This also provides management visibility. As NIS2 holds management accountable, they require understandable, real-world data on security performance (European Union, 2022). Providing executives with tangible evidence - such as the fact that all critical backups were successfully restored in testing, or that incident response drills consistently meet the 24h reporting window - translates technical compliance into business terms. Tools and approaches that aggregate security metrics into accessible forms (e.g., the Software Product Health Assistant (Strüwer et al., 2025), which presents software security status to decision-makers) exemplify how evidence can be made legible to non-technical stakeholders. The framework adopts this principle: each control is paired with evidence that serves internal improvement and also regulatory accountability. And a related observation from the product security literature is that decision-makers do not lack interest in security; rather, they more often lack legible, low-noise signals that translate risk into operational consequences (Strüwer et al., 2025).

Second, by focusing on cognitive load, the framework implicitly prioritizes certain NIS2 measures over others. The research concentrates on areas where human workload and behavior are decisive factors - incident reporting, training, daily "hygiene" practices, etc. This complements other emerging NIS2 models that operate at various levels. Recent high-level resilience models (Ristvej et al., 2025; Seeba et al., 2025) provide structural guidance but often abstract away from on-the-ground usability. The contribution of this research is to fill that gap by zooming in on the microlevel: how SME employees experience a given level of control in the flow of their work. For example, a preliminary, informal survey of 5 SME IT administrators revealed that incident reporting procedures scored an average of 70/100 to 80/100 on the Temporal Demand and the Frustration scale, suggesting these tasks are prime candidates for automation. This perspective is user-relevant and risk-relevant because controls aligned with operational routines are more likely to remain effective than controls that rely on sustained vigilance under time pressure.

Finally, the implications for SME contexts are significant: prioritize controls that are both effective and workable. Cybersecurity measures should be judged not just by theoretical coverage of risks, but by how they perform under real conditions - night shift, system fault, rush hour, or any scenario where personnel must act. Engineering interventions that align with operational routines shift compliance from documentation toward functional resilience. In practice, this might mean choosing a slightly less "perfect" technical control if it is dramatically more user-friendly, or allocating resources to iterative training rather than one-off sessions. These operator-oriented choices can reduce the likelihood of silent failures (controls that exist on paper but are circumvented in reality) and can build a safety culture where compliance is

seen as part of normal operations, not an added tax on productivity. Also, a specific cognitive friction point identified is the divergence between IT and Operational Technology (OT). Standard compliance frameworks often assume an IT-centric worldview (e.g., patching immediately), which conflicts with OT mandates for availability and safety. The framework addresses this by including OT assets already in the first phase (Baseline and Context Analysis), thereby reducing the cognitive dissonance operational staff face when forced to apply office security rules to industrial control systems.

## CONCLUSION

Latvian SMEs face an NIS2 compliance dilemma: controls comparable to those of larger enterprises are expected under limited cognitive and organizational capacity. This paper frames compliance as a cognitive- ergonomic design problem for work systems. Using a structured workload modelling approach informed by recent literature and SME practice, we propose a four-phase human-centric compliance framework that translates key NIS2 risk-management requirements under Article 21(2) into low-friction implementation steps. The analysis indicates that sustainable compliance depends on work-system fit: controls must reduce response effort, temporal pressure, and frustration, or they will be replaced by informal workarounds. Thus, the proposed approach is a practical way to "ground" NIS2 implementation for Latvian SMEs: it shifts compliance from formal policies into the domain of work-system engineering, where secure behavior becomes the simplest and most natural action within daily workflows. Of special note is the linkage between NKDL/NIS2 requirements and measurable workload indicators (NASA-TLX), which can support not only the implementation of controls but also active management of their "human cost." This allows organizations to systematically reduce friction points that most often lead to workarounds, silent incidents, and security fatigue.

The value of the "Starter Pack" is enhanced by mapping each requirement to concrete audit artifacts, ensuring both managerial control and regulatory transparency and reducing the risk of "paper compliance." In the SME context, this is critical: resources are limited, and effectiveness is determined not by the number of documents, but by the system's ability to function reliably under pressure (time constraints, staff turnover, night shifts, emergency situations). Therefore, the focus on secure-by-default mechanisms, short, role-based instructions, automated nudges, and regular, lightweight testing of recovery and response processes represents a viable path to sustainable NIS2 compliance that genuinely strengthens cyber resilience rather than fulfilling formal requirements.

Given the sectoral scope of NIS2, the proposed approach is relevant beyond the SME boundary. The framework for cognitive workload and evidence-driven governance may also be applicable to critical infrastructure and defense-grade cybersecurity contexts.

The framework is theoretically derived and requires empirical validation; field evaluation is planned as part of the authors' doctoral research program (pilot validation targeted for 2027).

## ACKNOWLEDGMENT

This research was partially supported by LLC Stratex (Latvia-Ukraine) and the University of Latvia.

## REFERENCES

Aksu, Ş.H., Adem, A., Çakıt, E., Dağdeviren, M., Karwowski, W. (2025). An examination of the interrelationships among NASA-TLX dimensions utilizing the DEMATEL method. PLoS ONE 20(4), e0320638.

Alomari, M.A., Al-Andoli, M.N., Ghaleb, M., *et al.* (2025). Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. *Energies, 18*(1), 141. DOI: 10.3390/en18010141.

Boyens, J., Paulsen, C., Bartol, N., Winkler, K., *et al.* (2022). *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Rev. 1 Update 1)*. National Institute of Standards and Technology, U.S. Dept. of Commerce. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf (Accessed: 4 February 2026)

Cabinet of Ministers of the Republic of Latvia (2025) Minimum Cybersecurity Requirements (Cabinet Regulation No. 397) [in Latvian], adopted 17 October 2025. Available at: https://likumi.lv/ta/id/361481 (Accessed: 24 January 2026).

Desolda, G., Greco, F., Lanzilotti, R., and Tucci, C. (2025). MORPHEUS: A multidimensional framework for modeling, measuring, and mitigating human factors in cybersecurity. *arXiv*, 2512.18303. Available at: https://arxiv.org/abs/2512.18303.

ENISA (2025a). *Cybersecurity Roles and Skills for NIS2 Essential and Important Entities: Mapping NIS2 Obligations with ECSF Role Profiles*. Available at: https://www.enisa.europa.eu/sites/default/files/2025-06/Mapping%20NIS%202%20obligations%20with%20ECSF%20role%20profiles.pdf (Accessed: 4 February 2026).

ENISA (2025b). *ENISA Threat Landscape 2025*. Version 1.2, October 2025. Available at: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf (Accessed: 15 January 2026).

ENISA (2025c). *NIS Investments 2025 – Main Report*. December 2025. Available at: https://www.enisa.europa.eu/sites/default/files/2025-12/NIS%20Investments%202025%20-%20Main%20report.pdf (Accessed: 4 February 2026).

ENISA (2025d). *Technical Implementation Guidance on Cybersecurity Risk-Management Measures*. Version 1.0, June 2025. Available at: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf (Accessed: 1 February 2026).

European Union (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, L 333, 27.12.2022, pp. 80–152. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 (Accessed: 4 February 2026).

Hadlington, L., and Ryding, C. (2026). *Human Factors and Cybersecurity: The Psychology of Online Safety and Security.* London: Routledge.

Khadka, K., and Ullah, A.B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security, 24*, Article 119. DOI: 10.1007/s10207-025-01032-0.

Kiran, U., Khan, N.F., Murtaza, H., Farooq, A., and Pirkkalainen, H. (2025). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. *Computers & Security, 149*, 104204. DOI: 10.1016/j.cose.2024.104204.

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *Holistica - Journal of Business and Public Administration, 13*(1), 49–72. DOI: 10.2478/hjbpa-2022-0003.

Nobles, C., and Robinson, N. (2024). The Missing Engineering Discipline in Cybersecurity: Human Factors Engineering. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 68*(1), 226–230.

Pramod, D. (2024). Gamification in cybersecurity education: A state of the art review and research agenda. Journal of Applied Research in Higher Education (2024). DOI: 10.1108/JARHE-02-2024-0072.

Ristvej, J., Tonhauser, M., Chovanec, D., Kubás, J., Kollár, B., and Zamiar, Z. (2025). Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. *Scientific Reports, 15*, 26902. DOI: 10.1038/s41598-025-12829-3.

Saeima of the Republic of Latvia (2024) National Cyber Security Law [in Latvian], adopted 10 November 2022, in force 1 January 2024. Available at: https://likumi.lv/ta/id/353390 (Accessed: 2 February 2026).

Seeba, M., Oja, T., Mäses, S., Murumaa, M., and Matulevičius, R. (2025). Toward NIS2 compliance for multiple stakeholders with security level evaluation framework. *Complex Systems Informatics and Modeling Quarterly, 45*, 136–159. Available at: https://csimq-journals.rtu.lv/article/view/csimq.2025-45.07/295 (Accessed: 14 January 2026).

Stouffer, K., Lightman, S., Abrams, M., *et al.* (2023). *Guide to Operational Technology (OT) Security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf. (Accessed: 7 January 2026)

Strüwer, J.-N., Trentinaglia, R., Wohlers, B., Bodden, E., and Dumitrescu, R. (2025). Assessing and communicating software security: Enhancing software product health with architectural threat analysis. In D. de Waal (Ed.), *Proceedings of the AHFE 2025 International Conference on Human Factors in Cybersecurity* (Vol. 168, pp. 82–92). Cham: Springer. DOI: 10.54941/ahfe1006145.

Tan, D. Jia Jun, Rafsanjani, A.S., Aslam, S., and Behjati, M. (2025). Human factors in information security: A quantitative study with technical solutions to prevent social engineering attacks. *Digital Threats: Research and Practice, 6*(4), 1–35. DOI: 10.1145/3767320.

Tet (2022). *Mazie un vidējie uzņēmumi apdraud sevi, uzskatot, ka kiberdrošība nav aktuāla* ["Small and medium enterprises endanger themselves by assuming cybersecurity is not relevant"]. Press release, 6 January 2022. Available at: https://www.tet.lv/par-tet/par-mums/jaunumi/mazie-un-videjie-uznemumi-apdraud-sevi-uzskatot-ka-kiberdrosiba-nav-aktuala (Accessed: 1 February 2026)

Verizon (2025). *2025 Data Breach Investigations Report (DBIR) - Executive Summary.* Available at: https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf (Accessed: 19 January, 2026)

Wachnik, R., Chruzik, K., and Pochopień, B. (2025). Sensor-based cyber risk management in railway infrastructure under the NIS2 Directive. *Sensors, 25*(23), 7384. DOI: 10.3390/s25237384.