Human Factors in Cybersecurity, Vol. 208, 2026, 117–129
https://doi.org/10.54941/ahfe1007418

Beyond Security Awareness: A Scoping Review of Human Factors in SME Cyber Resilience Frameworks (2018-2026)

Jonathan Thelen

Quality Science, Institute of Machine Tools and Factory Management, Technische Universität Berlin, 10587 Berlin, Germany

ABSTRACT

Small and medium-sized enterprises (SMEs) face cyber-attacks with disproportionate impact and limited capacity, yet the human-factors (HF) dimension of cyber resilience for this population remains methodologically heterogeneous. This scoping review maps how cyber resilience and cybersecurity frameworks for SMEs published between January 2018 and May 2026 operationalize HF constructs. Following PRISMA-ScR, we identified 482 records from four databases (Scite, Elicit, OpenAlex, Semantic Scholar) via twelve productive searches, including both keyword-style queries and an apples-to-apples replay of the same Scite Boolean strings on the keyword-indexed engines. After deduplication we screened 345 unique titles, assessed 126 for full-text eligibility, and synthesized 52 chart-eligible frameworks. To address abstractonly-charting risk, all 52 frameworks were read in full text and the coding re-validated against the original PDF. Security awareness dominates the SME HF lexicon (40/52, 77%); decision support (52%) and behavior change (44%) follow at moderate distance. Usability evaluation (12%), incident-response HF (13%), explicit technology acceptance (10%), trust modeling (10%), and cognitive workload (4%) remain underrepresented. Operationalization skews toward narrative process descriptions and single-item markers; metric-level operationalization and validated interventions are rare. We conclude with a research agenda for HF-explicit SME cyber resilience frameworks.

Keywords: Cyber resilience, SMEs, Human factors, Scoping review, Cybersecurity framework, Usability, Technology acceptance, Trust

INTRODUCTION

Cybersecurity has been recast over the last decade from a purely technical discipline into a sociotechnical one in which human factors (HF) codetermine the resilience of a digital organization. Interdisciplinary reviews argue that user behavior, decision-making, organizational culture, and trust-mediated interaction with security tools shape both vulnerabilities and resilience capacity (Van Der Kleij and Leukfeldt, 2020). For small and medium-sized enterprises (SMEs), the case is sharper: SMEs make up a structural backbone of European economies, are targeted by the same attack classes as large enterprises, and yet face capacity constraints that make mainstream frameworks such as NIST CSF or ISO/IEC 27001 disproportionate (Calvo-Manzano et al., 2025; El-Hajj and Mirza, 2024; Garrone, 2025).

Received May 29, 2026; Revised June 10, 2026; Accepted June 29, 2026; Available online July 20, 2026

A growing body of literature responds to this asymmetry by proposing SME-specific cyber resilience or cybersecurity frameworks. These range from self-assessment tools (Carias et al., 2021), design-science-grounded artefacts (Calvo-Manzano et al., 2025), governance models for micro-SMEs under NIS2 (Garrone, 2025), to TAM-based adoption studies (Radzi et al., 2024) and human-centric AI ecosystems for cross-sector defence (Kioskli et al., 2026). What is missing, however, is a transparent map of how these frameworks operationalize HF constructs: which constructs they name, how they translate them into items, dimensions, metrics, or interventions, and whether the resulting operationalization is empirically validated. Without such a map, the SME research community risks reinventing overlapping awareness instruments while leaving usability, trust, and acceptance underspecified (Neri and Niccolini, 2025; Troublefield, 2025).

This paper presents a scoping review that maps HF operationalization across SME cyber resilience frameworks published between January 2018 and May 2026.

The remainder of this paper is structured as follows. Section 2 describes the PRISMA-ScR-compliant methodology. Section 3 reports the descriptive and thematic synthesis of the 52 chart-eligible frameworks. Section 4 situates the findings against the broader HF-in-cybersecurity literature and articulates the research gap. Section 5 closes with limitations and a future research agenda.

METHODS

We conducted a scoping review following the five-stage framework of Arksey and O'Malley (Arksey and O'Malley, 2005), refined by Levac et al. (Levac et al., 2010) and updated through the JBI scopingreview methodology (Peters et al., 2020), and reported per the PRISMA Extension for Scoping Reviews (PRISMA-ScR) (Tricco et al., 2018). A scoping review is appropriate when the goal is to map an emerging fragmented field rather than to aggregate effect estimates. Our JBI Population, Concept, Context (PCC) schema is: Population: SMEs per EU recommendation 2003/361/EC (≤ 250 employees, branch-agnostic); Concept: operationalization of HF constructs (security awareness, behavior, technology acceptance, usability, decision support, culture, trust, cognitive workload, incident-response HF) within cyber resilience or cybersecurity frameworks; Context: 2018-01 to 2026-05, peer-reviewed venues and institutional frameworks. The four databases were chosen to span both academic-search paradigms: Scite and Elicit, both LLM-augmented (smart-citation Boolean and semantic respectively), and OpenAlex and Semantic Scholar, both keyword indexed and freely API-accessible. Twelve productive searches were issued across the four databases on 01 May 2026 (search-date cutoff) following a two-step strategy. The primary phase used database-native query styles (Table 1): two Boolean queries on Scite, one semantic query on Elicit three keyword queries on OpenAlex, and two keyword queries on Semantic Scholar. The robustness phase replayed the two original Scite Boolean strings verbatim on OpenAlex and Semantic Scholar to disentangle stringeffects from indexing/ranking-effects. For each query we retrieved up to the top-50 ranked results (top-25 by Scite's API default, and between 19 and 83 on Semantic Scholar where Boolean strings

returned smaller batches), a high-relevance cutoff imposed deliberately to make the synthesis tractable for a single reviewer; the coverage implications of this cap are discussed in the Limitations. Records were included if they (a) addressed an explicit SME context (EU recommendation 2003/361/EC, ≤250 employees), (b) proposed a multielement framework rather than a single isolated tool, and (c) explicitly named and operationalized at least one HF construct. Preprints from arXiv and preprints.org were eligible under the same criteria. Screening was performed by the sole author in three sequential passes (title/abstract relevance, full-text PCC eligibility, Tier-A vs. Tier-B classification), followed by a full-text validation read of all 52 Tier-A papers as a within-author intracoder reliability check (see Section 5). Charting followed an a-priori scheme: framework label, HF construct(s), operationalization mode (one of: item for questionnaire items, dimension for top-level framework axis, metric for numerical score, intervention for training/tool action, process for procedural step, or mixed), validation, and contribution type. Frequency tabulation and thematic synthesis were applied without statistical aggregation per scoping-review convention. Figure 1 reports the PRISMA-ScR flow.

Table 1: Search strategy. All queries restricted to 1 January 2018 to 01. May 2026.

#	Database	Query (Boolean / Semantic / Keyword)	Hits
S1	Scite	*(cyber resilience* OR *cybersecurity framework* OR *information security management)* AND *(small and medium* OR SMEs OR SME) AND *(human factors* OR *usability* OR *acceptance* OR *user-centered)*	25
S2	Scite	*(cyber resilience OR cybersecurity framework OR information security management) AND (small and medium-sized enterprises OR SMEs) AND (security awareness OR behavioral change OR user-centered design OR technology acceptance OR UTAUT OR TAM)*	25
S3	Elicit	*Semantic:* How do cyber resilience and cybersecurity frameworks for SMEs operationalize human factors constructs (usability, acceptance, awareness, UCD, decision support)?	30
S4	OpenAlex	*cyber resilience* SME human factors (filter: type = article OR book-chapter OR proceedings)	50
S5	OpenAlex	*cybersecurity* SME UTAUT TAM acceptance	50
S6	OpenAlex	cybersecurity SME usability framework	50
S7	Sem. Scholar	cyber resilience SME human factors	25
S8	Sem. Scholar	cybersecurity SME technology acceptance UTAUT	25
S9	OpenAlex	S1 verbatim (Scite broad Boolean)	50
S10	OpenAlex	S2 verbatim (Scite specific Boolean)	50
S11	Sem. Scholar	S1 verbatim (Scite broad Boolean)	83
S12	Sem. Scholar	S2 verbatim (Scite specific Boolean)	19

After abstract-based charting, every Tier-A paper was read in full text against the chart entry, with every coding deviation from the abstract-based entry recorded with the paper-internal page anchor that justified the change. Two papers initially in Tier-A turned out to be cross-domain metric reviews rather than primary SME frameworks and were reclassified to Tier-B before the validation read. Of the 52 reads, four yielded clear coding refinements (the Antunes Portugal case-study lost the Behavior tag and gained IncidentResponse; the Doucek Czech/Slovak audit analysis lost Decision-Support; the Benz & Chatterjee CET and the SMESEC framework gained IncidentResponse). The remaining 48 re-reads confirmed the abstract-based coding. Across the full validation, additions outnumbered deletions roughly twoto one, consistent with the hypothesis that abstract-only scoping in this domain may undercount HF coverage, a caveat discussed further in the Limitations (Section 5). The validation also surfaced a recurring corpus pattern: HF constructs are frequently named in framework dimensions without being operationalized as items, scales, metrics, or interventions, which underpins the under-operationalization argument in the Discussion. As a robustness check, source-attribution analysis confirmed that the four-database design captures genuinely complementary slices of the literature: 52% of Tier-A papers were retrieved only by the keyword-indexed engines, 21% only by the LLM-augmented engines, and only 27% by both paradigms.

RESULTS

Descriptive overview The 52 chart-eligible frameworks span January 2018 to May 2026 with publication acceleration after 2023. Categories are non-exclusive: conceptual contributions (n = 27), empirical studies (n = 18, largest the Cyberpsychology mixed-methods study with n = 523 employees across 78 SMEs (Troublefield, 2025)), tool-centered contributions (n = 12), and reviews (n = 3 in TierA; two further review-style papers were re-classified to Tier-B during the full-text validation). The corpus is European-leaning (22 of 52; 11 Americas/global, 9 Asia-Pacific, 10 MENA/SSA), cross-sectoral (39 generic, 13 sector-specific), and predominantly journal/conference (28+18).

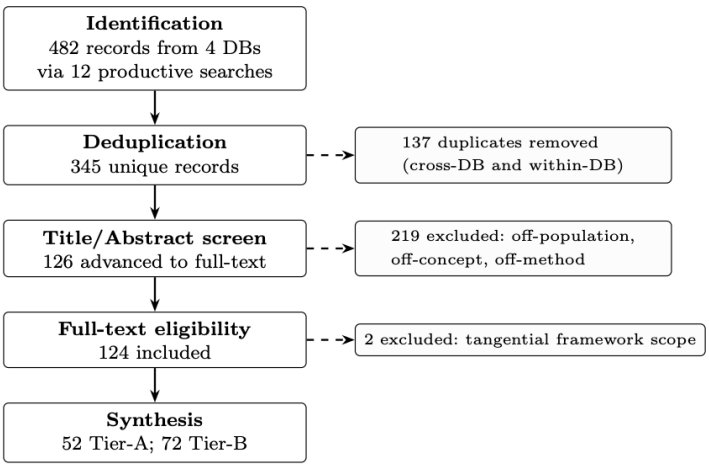

Figure 1: PRISMA-ScR flow.Tier A = chart-eligible (SME + operationalized HF construct); Tier B = contextual or theoretical anchors.

Construct frequencies across the 52 charted frameworks cleave the corpus into a dominant cluster and an under-operationalized tail. Security awareness is present in 40 of 52 (77%), the de-facto lingua franca; Decision support (27/52, 52%) and behavior change (23/52, 44%) follow at substantial distance. Both were strengthened by the full-text validation pass, which surfaced DS-operationalization in CR-SAT, CYSEC, El-Hajj CSRAF, the UEBA SME framework, the integrated SME information security governance framework (Mwanje et al., 2023), the Welsh-SME ROHAN model (Rawindaran et al., 2025), and the Cyber Resilient Behavior framework (Van Der Kleij and Leukfeldt, 2020). Organizational culture (13/52, 25%) appears mainly in 2023 to 2026 frameworks emphasizing socio-technical resilience. The picture inverts for the lower half. Usability is operationalized in 6 of 52 (12%): only CYSEC (Shojaifar and Fricker, 2023) runs iterative formative usability evaluation; the SMESEC H2020 framework (Cucurull et al., 2020) integrates user-facing tutorials; design-desideratum mentions appear in CyberESP, the Human-Centric AI Ecosystem, the DigitAll Reality HCI survey and the generative-AI SME framework (Calvo-Manzano et al., 2025; Kioskli et al., 2026; Szücs et al., 2025; Awan et al., 2026); none applies the SUS, think-aloud, or established UX methods to its own artefact recurrently. Technology acceptance through TAM/UTAUT-related models appears in 5 of 52 (10%) (Radzi et al., 2024; Kioskli et al., 2026; Yawised et al., 2025; Dighriri et al., 2025; AL-Dosari and Fetais, 2023), but no Tier-A framework embeds a full UTAUT instrument as a lifecycle step. Trust modeling is present in 5 of 52 (10%). It shows up as an inter-organizational structural precondition in collaborative resilience (Mmango and Gundu, 2024; Ngandu et al., 2026), as a DSS-component framing in CR-SAT (Carias et al., 2021) and PALANTIR (Mlakar et al., 2021), and as the focus of confidentiality concern surveys (Shojaifar and Fricker, 2020). However, no framework in the corpus operationalizes trust calibration as a measurement. Incidentresponse HF appears in 7 of 52 (13%, strengthened by the full-text validation read which surfaced explicit IR layers in Antunes Portugal (ISO 27001 A.16) (Antunes et al., 2021), Benz & Chatterjee CET (Benz and Chatterjee, 2020), and SMESEC (Cucurull et al., 2020) alongside Cyberpsychology, Cyber Resilient Behavior (Van Der Kleij and Leukfeldt, 2020), CR-SAT and PALANTIR), none implementing explicit role-clarity or communication protocol evaluation. Cognitive workload is operationalized in only 2 of 52 (4%): the manager security-related-stress study (Chen et al., 2026) via self-report, and the Cyberpsychology ISCPM's Cognitive-Resource Interface (Troublefield, 2025). No NASA-TLX or dual-task application was found, making workload the most under-operationalized construct in the SME corpus.

Construct × mode coverage. Figure 2 cross-tabulates the nine PCC HF constructs against the six operationalization modes. Of 54 possible cells, 38 are populated; the 16 empty cells locate the most actionable HF research opportunities. Awareness covers all six modes; Usability appears only in Process, Item, and Intervention; Acceptance only in Item, Mixed, and Process; Cognitive Workload only in Item.

HF construct \ Op. mode	Proc.	Item	Dim.	Metr.	Mix.	Interv.
Awareness	14	7	9	3	5	2
Behavior	4	7	4	1	5	2
Decision sup.	14	4	3	3	2	1
Culture	4	·	4	1	4	·
Usability	4	1	·	·	·	1
Trust	1	2	1	·	1	·
Acceptance	1	3	·	·	1	·
Incident resp.	3	2	1	·	1	·
Cog. workload	·	1	·	·	1	·

Figure 2: HF construct × operationalization mode across the 52 T r-A frameworks (max cell value = 14). Op. mode abbreviations (defined inline in Section 2): Proc. = Process, Item, Dim. = Dimension, Metr. = Metric, Mix. = Mixed, Interv. = Intervention. Cells marked · are construct/mode combinations not operationalized in any charted framework; the empty cells are the most actionable HF research opportunities for SME cyber resilience.

DISCUSSION

The dominant pattern is the over-reliance on "security awareness". 40 of 52 frameworks (77%) name awareness explicitly, often as the sole HF construct present. This pattern is robust to the database expansion, since both the keyword and the same-string Boolean replays produce only singlepercentage point shifts. The awareness monoculture therefore reflects a structural feature of the SME literature, not a search artefact. It aligns with the NIS2 awareness-first framing (Garrone, 2025) but contrasts sharply with the broader HF-in-cybersecurity discourse, where multidimensional schemes are already established (Desolda et al., 2025; Khadka and Ullah, 2025; Naqvi et al., 2021; Grobler et al., 2021). The usability, acceptance and trust gap documented in Section 3 (each construct at or below 12%) is the most actionable finding, and adjacent reviews report analogous gaps in user-centric cybersecurity studies (Tari and Mahmud, 2025; Hakimi et al., 2024).

Table 2. Charting matrix of the 52 Tier-A SME cyber resilience frameworks. HF codes: AW = Awareness, BH = Behavior, DS = Decision Support, CU = Culture, US = Usability, TR = Trust, AC = Acceptance, IR = Incident Response, CW = Cognitive Workload. Op. mode: Item, Dimension, Metric, Intervention, Process, Mixed (defined inline in Section 2). Validation: Conc. = Conceptual, Surv. = Survey, Case = Case study, Int. = Interview, Wkshp = Workshop, Emp. = Empirical, Tut. = Tutorial, DSR = DesignScience Research, MLR = Multivocal LR, Pol. = Policy analysis. Source: Sc = Scite, EI = Elicit, OA = OpenAlex, S2 = Semantic Scholar.

Ref.	HF Constructs	Op. mode	Validation	Source
Venkatesh (2018)	DS AW	Item	Conc.+Tool	OA,S2
Van Der Kleij and Leukfeldt (2020)	BH AW IR DS	Dimension	Pilot n = 56	EI
Bada and Nurse (2019)	AW BH	Process	Conc.	Sc,OA
Ponsard et al. (2019)	AW	Item	Surv.	EI
Shojaifar and Fricker (2020)	BH TR	Item	Surv.	Sc,OA
Carias et al. (2020)	AW DS	Process	Case	Sc,EI,OA,S2
Benz and Chatterjee (2020)	DS AW IR	Item	Conc.+Tool	OA,S2
Douchek et al. (2020)	AW	Dimension	Audit n = 440	OA,S2
Cucurull et al. (2020)	AW DS US IR	Process	DSR+Tut.	OA,S2
Shojaifar and Järvinen (2021)	AW	Dimension	Wkshp.	Sc
Carias et al. (2021)	AW DS IR TR	Item	DSR+Case+Exp	Sc,EI,OA
Antunes et al. (2021)	AW IR	Process	Case	OA
Löffler et al. (2021)	AW BH	Intervention	Pilot	OA
Mlakar et al. (2021)	DS IR TR	Process	Conc.+UC	OA
Romaniuk and Shuprudko (2021)	AW BH	Dimension	Emp.	OA,S2
Pawar and Palivela (2022)	AW DS	Process	Conc.	OA
Yigit Ozkan and Spruit (2023)	AW DS	Dimension	Conc.	OA
Mmango and Gundu (2023)	AW CU	Dimension	Conc.	EI,S2
Marican et al. (2023)	AW CU	Dimension	Meta	Sc
Asprion et al. (2023)	DS AW	Process	Expert	EI
Shojaifar and Fricker (2023)	US AW BH DS	Intervention	Surv.+Int.	Sc
AL-Dosari and Fetais (2023)	AW AC	Mixed	Meta	Sc,OA
Mwanje et al. (2023)	AW DS CU	Process	Conc.	S2
Saar and Dagada (2024)	AW CU	Process	Surv.	Sc
Mmango and Gundu (2024)	BH TR CU	Dimension	Conc.	EI
El-Hajj and Mirza (2024)	AW DS BH	Process	Pilot	Sc,OA
Radzi et al. (2024)	AC BH	Item	Surv.	Sc,OA
Hoong et al. (2024)	BH CU	Mixed	Int. n = 46	OA

(Continued)

Table 2: Continued.

Ref.	HF Constructs	Op. mode	Validation	Source
Ludin et al. (2024)	AW DS	Dimension	Meta-Comp.	OA,S2
Calvo-Manzano et al. (2024)	AW DS	Mixed	Conc.	OA
Klitis et al. (2024)	AW CU	Process	Conc.	S2
Le et al. (2025)	BH DS AW	Metric	Conc.	EI,S2
Deruma (2025)	AW DS CU	Metric	Expert	EI,OA,S2
Calvo-Manzano et al. (2025)	DS US	Process	DSR+Case	Sc,S2
Rusu and Mantulescu (2025)	AW DS	Process	Conc.	Sc,OA,S2
Neri and Niccolini (2025)	AW BH CU	Mixed	Surv.+Int.	EI,OA,S2
Garrone (2025)	AW DS BH	Process	Pol.+Emp.	Sc,S2
Szücs et al. (2025)	AW US BH	Item	Surv.	EI
Troublefield (2025)	BH CU AW DS CW IR	Mixed	Mixed n = 523	EI
Rawindaran et al. (2025)	AW CU BH DS	Process	Mixed Surv+Int	OA,S2
Pawan and T (2025)	DS AW	Process	Conc.	OA
Bahmanova and Lace (2025)	DS AW	Metric	Conc.	S2
Yawised et al. (2025)	AC BH	Item	Surv.	S2
Metropolitan Consulting Group et al. (2025)	AW DS	Item	Surv. n = 44	S2
Orellana (2025)	CU BH	Mixed	Surv.+Case	S2
Dighriri et al. (2025)	AC BH	Item	Surv.+SEM	S2
Lasi (2025)	AW BH	Item	Surv. n = 240	S2
Kioskli et al. (2026)	US AC DS	Process	X-sect.	EI
Ngandu et al. (2026)	BH TR AW	Mixed	Conc.	OA
Sithole et al. (2026)	AW BH CU	Dimension	Qual.	S2
Awan et al. (2026)	DS US	Process	MLR	S2
Chen et al. (2026)	BH CW	Item	Surv.	S2

Operationalization in the corpus is predominantly narrative-process or single-item; only two frameworks offer intervention-with-measurableoutcomes designs (Shojaifar and Fricker, 2023; Löffler et al., 2021), and conceptual artefacts without empirical validation form the modal pattern, a sign of an early generative phase. Three implications follow for the next generation of HF-explicit SME frameworks: (i) the competitive advantage lies in operationalizing usability, acceptance, and trust simultaneously rather than refining yet another awareness instrument; (ii) methodological credibility will depend on metric- or intervention-level operationalization with empirical validation; (iii) the small subset of design-science-grounded artefacts (Calvo-Manzano et al., 2025; Carias et al., 2021; Shojaifar and Fricker, 2023) provides a template: artefact-centered, iteratively validated, HF-explicit.

CONCLUSION

This scoping review of 52 SME cyber resilience frameworks (January 2018 to May 2026), drawn from four academic databases via twelve productive searches and supplemented by a structured full-text validation pass over all 52 Tier-A frameworks, finds a security-awareness monoculture (77%) coexisting with substantial decision-support (52%) and behaviorchange (44%) operationalization. By contrast, incident-response HF (13%), usability evaluation (12%), technology acceptance (10%), trust modeling (10%), and cognitive workload (4%) remain underrepresented. The construct distribution is robust to the database expansion: both the keyword-style additions and the apples-to-apples same-string replay produce only single-percentage-point shifts. Operationalization is predominantly narrative-process or single-item, with rare metric-level or intervention designs. Three implications follow: treat usability, acceptance and trust as co-equal with awareness; shift toward design-science artefact evaluation; pursue multi-construct frameworks combining awareness, behavior, decision support, and trust within one coherent operationalization. For the AHFE Human Factors in Cybersecurity community, SME cyber resilience is a domain where classic HF methodology (SUS, UTAUT, think-aloud, trust calibration, NASA-TLX) has yet to be systematically applied to the framework artefact itself. One immediate application of this gap analysis is the German CyResNet research initiative (Cyber Resilience Framework and Network for SMEs, 2026 to 2028), in which an HF-explicit framework adapted from EFQM 2020 is currently under development to address exactly the usability, acceptance and trust gap documented here.

Three caveats apply. (i) Single-reviewer title/abstract and full-text screening; an intra-coder reliability estimate is available (the full-text validation read confirmed the abstract-based codings on 48 of 52 TierA papers, 92.3% agreement, with four page-anchored refinements), but a formal inter-coder reliability assessment against an independent second coder remains future work. (ii) The top-50-per-query sampling cap bounds coverage of broad Boolean strings that can return thousands of hits per database; the synthesis therefore reflects high-relevance ranked results rather than the full retrievable corpus. (iii) Three central references (ElHajj and Mirza, 2024; Garrone, 2025; Desolda et al., 2025) are preprints and have not yet undergone peer review.

REFERENCES

AL-Dosari, K. and Fetais, N. (2023), 'Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach', Electronics 12(17), 3629.

Antunes, M., Maximiano, M., Gomes, R. and Pinto, D. (2021), 'Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal', Journal of Cybersecurity and Privacy 1(2), 219– 238.

Arksey, H. and O'Malley, L. (2005), 'Scoping studies: Towards a methodological framework', International Journal of Social Research Methodology 8(1), 19–32.

Asprion, P., Gossner, P. and Schneider, B. (2023), Cybersecurity Governance – An Adapted Practical Framework for Small Enterprises.

Awan, M., Alam, A., Khan, R. A., Alwageed, H. S., Ayouni, S. and Almagrabi, A. O. (2026), 'A generative AI-driven cybersecurity framework for small and medium enterprises software development: An ANN-ISM approach', Scientific Reports 16(1), 9813.

Bada, M. and Nurse, J. R. (2019), 'Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)', Information & Computer Security 27(3), 393–410.

Bahmanova, A. and Lace, N. (2025), Aligning SME Critical Assets with Cyber Risks Using a Matrix Model to Develop a Cyber Resilience Framework, pp. 436–444.

Benz, M. and Chatterjee, D. (2020), 'Calculated risk? A cybersecurity evaluation tool for SMEs', Business Horizons 63(4), 531–540.

Calvo-Manzano, J. A., San Feliu, T., Herranz, A., Mariño, J., Fredlund, L.-A., Colomo-Palacios, R. and Moreno, A. M. (2024), Towards an Integrated Cybersecurity Framework for Small and Medium Enterprises, in M. Yilmaz, P. Clarke, A. Riel, R. Messnarz, C. Greiner and T. Peisl, eds, 'Systems, Software and Services Process Improvement', Vol. 2179, Springer Nature Switzerland, pp. 231–244.

Calvo-Manzano, J. A., San Feliu, T., Herranz, A., Mariño, J., Fredlund, L.-A. and Moreno, A. M. (2025), 'CyberESP: An Integrated Cybersecurity Framework for SMEs', Journal of Software: Evolution and Process 37(9), e70050.

Carias, J. F., Arrizabalaga, S., Labaka, L. and Hernantes, J. (2021), 'Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs', IEEE Access 9, 80741–80762.

Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S. and Hernantes, J. (2020), 'Systematic Approach to Cyber Resilience Operationalization in SMEs', IEEE Access 8, 174200–174221.

Chen, H., Fan, J. and Lyu, T. (2026), 'Manager information security-related stress and organizational information security performance', Management Decision pp. 1–30.

Cucurull, J., Tselios, C., Rueda, C., Folch, N., Copty, F., Igbaria, R., Athanatos, M., Krithinakis, A., Ioannidis, S., Ruiz, J. F. and Barrientos, P. (2020), Integration of an online voting solution with the SMESEC security framework, in '2020 IEEE International Systems Conference (SysCon)', IEEE, pp. 1–8.

Deruma, S. (2025), 'Cyber Resilience Key Metrics in Small and Medium-Sized Enterprises', Economics Ecology Socium 9(1), 15–23.

Desolda, G., Greco, F., Lanzilotti, R. and Tucci, C. (2025), 'MORPHEUS: A Multidimensional Framework for Modeling, Measuring, and Mitigating Human Factors in Cybersecurity'.

Dighriri, A. A. M., Chatrath, S. K. and Mohammadian, M. (2025), 'Exploring Determinants of Information Security Systems Adoption in Saudi Arabian SMEs: An Integrated Multitheoretical Model', Journal of Cybersecurity and Privacy 5(4), 113.

Douchek, P., Nedomova, L., Luc, L. and Novak, L. (2020), Information Security: The Glory and Penury of SMEs in the Czech and Slovak Republics, in '2020 International Conference on Engineering Management of Communication and Technology (EMCTECH)', IEEE, pp. 1–7.

El-Hajj, M. and Mirza, Z. A. (2024), 'Protecting Small and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool'.

Garrone, R. (2025), 'Proportionate Cybersecurity for Micro-SMEs: A Governance Design Model under NIS2'.

Grobler, M., Gaire, R. and Nepal, S. (2021), 'User, Usage and Usability: Redefining Human Centric Cyber Security', Frontiers in Big Data 4, 583723.

Hakimi, M., Mohammad Mustafa Quchi and Abdul Wajid Fazil (2024), 'Human factors in cybersecurity: An in depth analysis of user centric studies', Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID) 3(01), 20–33.

Hoong, Y., Rezania, D. and Baker, R. (2024), 'When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands', Technology in Society 78, 102650.

Khadka, K. and Ullah, A. B. (2025), 'Human factors in cybersecurity: An interdisciplinary review and framework proposal', International Journal of Information Security 24(3), 119.

Kioskli, K., Seralidou, E., Mallouli, W., Koutras, D., Tomás, P. and Kallergis, D. (2026), 'A HumanCentric AI-Enabled Ecosystem for SME Cybersecurity: Cross-Sectoral Practices and Adaptation Framework for Maritime Defence', Electronics 15(7), 1520.

Klitis, C., Makris, I., Bouzinis, P., Asimopoulos, D. C., Mallouli, W., Kioskli, K., Seralidou, E., Douligeris, C. and Christofi, L. (2024), NERO: Advanced Cybersecurity Awareness Ecosystem for SMEs, in 'Proceedings of the 19th International Conference on Availability, Reliability and Security', ACM, pp. 1–9.

Lasi, M. B. A. (2025), 'Understanding cybersecurity awareness in Malaysian SMEs: The role of knowledge, resources, experience, and policy', International Journal of Asian Social Science 15(9), 245– 256.

Le, T. D., Le Dinh, T. and Uwizeyemungu, S. (2025), 'A cybersecurity framework for enhancing Small and medium-sized enterprises (SMEs) security posture using user behaviour analytics', Enterprise Information Systems 19(10), 2529282.

Levac, D., Colquhoun, H. and O'Brien, K. K. (2010), 'Scoping studies: Advancing the methodology', Implementation Science 5(1), 69.

Löffler, E., Schneider, B., Zanwar, T. and Asprion, P. M. (2021), 'CySecEscape 2.0: A Virtual Escape Room To Raise Cybersecurity Awareness', International Journal of Serious Games 8(1), 59–70.

Ludin, W. N. E. W. M., Mohd, M. and Paizi@Fauzi, W. F. (2024), 'Comparative Analysis of Small and Medium-Sized Enterprises Cybersecurity Program Assessment Model', International Journal of Advanced Computer Science and Applications 15(8).

Marican, M. N. Y., Razak, S. A., Selamat, A. and Othman, S. H. (2023), 'Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review', IEEE Access 11, 5442–5452.

Metropolitan Consulting Group, Agyapong, K., Boakye, I. and Accra Institute of Technology (2025), 'An Assessment of the Effect of Information Security Management System on Organisational Performance', International Journal of Multidisciplinary Research and Analysis 08(03).

Mlakar, I., Jeran, P., Safran, V. and Logothetis, V. (2021), A Cost-Effective Security Framework to protect micro enterprises: PALANTIR e-commerce use case, in '2021 9th International Symposium on Digital Forensics and Security (ISDFS)', IEEE, pp. 1–6.

Mmango, N. and Gundu, T. (2023), Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs, in '2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)', IEEE, pp. 1–6.

Mmango, N. and Gundu, T. (2024), 'Cultivating Collective Armor: Towards a Collaborative Cybersecurity Resilience Framework for SMEs', European Conference on Innovation and Entrepreneurship 19(1), 523–531.

Mwanje, D., Samuel, O., Tumwebaze, G. and Bukenya, M. (2023), 'A Framework to Enhance Information Security Governance in SMEs', Saudi Journal of Engineering and Technology 8(12), 300–303.

Naqvi, B., Clarke, N. and Porras, J. (2021), 'Incorporating the human facet of security in developing systems and services', Information & Computer Security 29(1), 49–72.

Neri, M. and Niccolini, F. (2025), 'On the path to cyber organizational resilience: Shedding light on the context of SMEs', International Journal of Organizational Analysis 33(12), 105–131.

Ngandu, M. R., Mabanza, N. and Mwansa, G. (2026), Enabling SME Participation in Cybersecurity Information Sharing: A Human-Centric, Socio-Technical Model, in A. Iglesias, J. Shin, N. Bhatt and A. Joshi, eds, 'Information Systems for Intelligent Systems', Vol. 1756, Springer Nature Switzerland, pp. 148–157.

Orellana, F. (2025), 'Assessing Cybersecurity Response Readiness and Return on Security Investment Strategies among SMEs in Ecuador', Global Journal of Computer Science and Technology pp. 27–32.

Pawar, S. and Palivela, D. H. (2022), 'LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)', International Journal of Information Management Data Insights 2(1), 100080.

Pawar, S. and T, J. (2025), 'Implementing HIPAA Compliant Cybersecurity for Healthcare SMEs using BDSLCCI Framework', European Economic Letters (EEL) 15(2), 883–903.

Peters, M. D., Marnie, C., Tricco, A. C., Pollock, D., Munn, Z., Alexander, L., McInerney, P., Godfrey, C. M. and Khalil, H. (2020), 'Updated methodological guidance for the conduct of scoping reviews', JBI Evidence Synthesis 18(10), 2119–2126.

Ponsard, C., Grandclaudon, J. and Bal, S. (2019), Survey and Lessons Learned on Raising SME Awareness about Cybersecurity:, in 'Proceedings of the 5th International Conference on Information Systems Security and Privacy', SCITEPRESS - Science and Technology Publications, pp. 558–563.

Radzi, N. R., Tajuddin, S. N. A. A. and Bahari, K. A. (2024), 'Small Steps, Big Security: TAM-Powered Insights of Cybersecurity Adoption Among Small-And-Medium Entrepreneurs in Digital Business', Journal of Ecohumanism 3(3), 1626–1638.

Rawindaran, N., Jayal, A. and Prakash, E. (2025), 'Cybersecurity Framework: Addressing Resiliency in Welsh SMEs for Digital Transformation and Industry 5.0', Journal of Cybersecurity and Privacy 5(2), 17.

Romaniuk, T. and Shuprudko, N. (2021), 'Determinants of success information security management of small and medium business', Bulletin of Chernivtsi Institute of Trade and Economics III(83), 79–90.

Rusu, D. and Mantulescu, M. (2025), 'Development of an Application-Based Framework for Information Security Management in SMEs', Sustainability 17(18), 8314.

Saar, G. and Dagada, R. (2024), 'Building Cybersecurity Capacities in Zambia's Business Sector: Guideline for SMEs', International Conference on Cyber Warfare and Security 19(1), 317–326.

Shojaifar, A. and Fricker, S. A. (2020), SMEs' Confidentiality Concerns for Security Information Sharing, in N. Clarke and S. Furnell, eds, 'Human Aspects of Information Security and Assurance', Vol. 593, Springer International Publishing, pp. 289–299.

Shojaifar, A. and Fricker, S. A. (2023), 'Design and evaluation of a self-paced cybersecurity tool', Information & Computer Security 31(2), 244–262.

Shojaifar, A. and Järvinen, H. (2021), Classifying SMEs for Approaching Cybersecurity Competence and Awareness, in 'Proceedings of the 16th International Conference on Availability, Reliability and Security', ACM, pp. 1–7.

Sithole, M., Odette, S. and Munzhelele, F. (2026), 'Cybersecurity challenges and a conceptualised maturity Typology in Ugandan SMEs: A qualitative analysis', International Journal of Business Ecosystem & Strategy (2687-2293) 8(1), 105–119.

Szücs, V., Ar´any, G. and D´avid, A. (2025), 'Security Awareness of HCI in DigitAll Reality', Acta Polytechnica Hungarica 22(6), 9–23.

Tari, Z. and Mahmud, R. (2025), 'Augmenting Digital Ecosystem Resilience Through Human-Centric Cybersecurity Solutions', IEEE Transactions on Engineering Management 72, 3892–3908.

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., Lewin, S., Godfrey, C. M., Macdonald, M. T., Langlois, E. V., Soares-Weiser, K., Moriarty, J., Clifford, T., Tunçalp, O. and Straus, S. E. (2018), 'PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation', Annals of Internal Medicine 169(7), 467–473.

Troublefield, T. C. (2025), 'The Cyberpsychology of Small and Medium-Sized Enterprises Cybersecurity: A Human-Centric Approach to Policy Development', Journal of Information Security 16(01), 158–183.

Van Der Kleij, R. and Leukfeldt, R. (2020), Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security, in T. Ahram and W. Karwowski, eds, 'Advances in Human Factors in Cybersecurity', Vol. 960, Springer International Publishing, pp. 16–27.

Venkatesh, V. (2018), 'Design of Cybersecurity Risk Assessment Tool for Small and Medium Sized Businesses using the NIST Cybersecurity Framework'. Yawised, K., Apasrawirote, D., Chatrangsan, M. and Muneesawang, P. (2025), 'Extending UTAUT2 towards acceptance by SMEs of the mobile application platform "Tripper Notifier Application"', Journal of Science and Technology Policy Management .

Yigit Ozkan, B. and Spruit, M. (2023), 'Adaptable Security Maturity Assessment and Standardization for Digital SMEs', Journal of Computer Information Systems 63(4), 965–987.