

Human Factors in Information Security and Technological Risk: A Systematic Literature Review

Kseniia Baimakova

Director of Professional Skills Development Center, Senior lecturer, International Entrepreneurship Chair, Institute of Entrepreneurship Technologies and Law
k.baimakova@gmail.com

Abstract: The increasing complexity and interconnectedness of digital technologies have transformed information security from a predominantly technical challenge into a broader socio-technical risk problem. Human behaviour, risk perception, trust, organisational conditions, and decision-making increasingly influence whether technological vulnerabilities translate into actual security consequences. This study systematically reviews recent research on the human dimensions of information security and technological risk, with particular attention to the relationships between technological vulnerabilities, perceived risk, trust, security-related decision-making, and behaviour. The review focuses on studies published between 2020 and 2026 and covers diverse technological contexts, including conventional information systems, mobile technologies, IoT, BYOD environments, autonomous systems, and critical infrastructures. The literature is synthesised into five interconnected themes: human factors and security behaviour; risk perception and security-related decision-making; trust and organisational security; technological risk, failure, and reliability; and cybersecurity challenges in critical infrastructures and emerging technologies. Based on this synthesis, the study proposes an Integrated Human-Centred Cybersecurity Risk Framework linking technological and contextual conditions to risk perception, trust and perceived control, security-related decisions, behaviour, and subsequent security and resilience outcomes. The review highlights the need for closer integration between technical risk assessment and behavioural and organisational approaches to information security.

Keywords: cybersecurity; human factors; technological risk; risk perception; trust; security behaviour

1 Introduction

The growing interconnectedness of digital technologies has transformed information security from a predominantly technical challenge into a socio-technical problem in which technological, behavioural, and organisational factors

interact [1], [2]. This is particularly evident in IoT and other complex digital environments, where technical safeguards cannot eliminate vulnerabilities associated with human behaviour [3]. Human factors can increase vulnerability through inadequate awareness or unsafe practices, but knowledge, appropriate decision-making, and supportive organisational conditions can also strengthen security and resilience [4]. A central challenge is the distinction between objective technological risk and subjective risk perception. Technical vulnerabilities and failures can be identified through engineering-oriented risk and reliability methods [5], but users' responses depend on how these risks are perceived and evaluated. Risk perception, trust, perceived control, and security-related decision-making therefore provide important mechanisms through which technological conditions are translated into actual security behaviour [6]. Despite increasing recognition of these relationships, the literature remains fragmented across technological and disciplinary contexts. Human-centred cybersecurity and organisational security are often examined separately from technological reliability, while risk perception and trust are conceptualised differently across conventional information systems, autonomous technologies, and critical infrastructures [7]. What remains insufficiently integrated is the process through which objective technological conditions, subjective risk appraisal, trust, and organisational factors jointly shape security-related decisions and outcomes across different technological contexts. To address this gap, this study systematically reviews 47 publications published between 2020 and 2026 on the human dimensions of information security and technological risk. It examines the relationships among technological vulnerability, risk perception, trust, perceived control, and security-related decision-making across different technological contexts. The review aims to identify recurring patterns, integrate technical and behavioural perspectives, reveal research gaps, and develop an Integrated Human-Centred Cybersecurity Risk Framework.

2 Conceptual Background

2.1 From Technological Vulnerability to Human-Centred Cybersecurity

Building on the socio-technical perspective, human-centred cybersecurity research emphasises users' cognitive characteristics, motivations, work practices, and organisational contexts [1], [2]. This is evident in IoT and healthcare environments, where human behaviour, awareness, organisational practices, and exposure to social-engineering threats remain important despite technical safeguards [3], [4]. Organisational and information-security cultures further influence employee compliance and security behaviour [8]. Human factors, however, are not

exclusively sources of vulnerability. Knowledge, awareness, effective decision-making, and supportive organisational conditions can strengthen security and resilience, reinforcing the view that human capabilities can also enhance cybersecurity [9]. Earlier research focusing on Generation Y similarly highlighted the relevance of user awareness and attitudes in information security, indicating that the human dimension of cybersecurity had already emerged as an important concern before the period covered by the systematic corpus [45]. BYOD environments illustrate this dual role particularly clearly: employee autonomy introduces security and governance challenges, while policy compliance and organisational responses require attention to both behavioural and managerial factors [10], [11]. Human factors should therefore be considered integral components of cybersecurity rather than external sources of error.

2.2 Risk Perception, Decision-Making, and Security Behaviour

Objective technological vulnerability does not automatically produce risky behaviour. Security responses depend on how users interpret threats through knowledge, perceived vulnerability, expected consequences, self-efficacy, and individual risk tendencies. Cybersecurity knowledge and personal characteristics are associated with security practices [12], while passive risk tendencies demonstrate that insecure outcomes may result from inaction rather than deliberate risk-taking [13]. Perceived vulnerability [14] and broader cognitive and motivational mechanisms [15] further influence whether technological threats lead to protective behaviour. Information-security policy compliance is likewise shaped by interacting motivational, self-regulatory, and deterrence mechanisms [16]. Password security illustrates this distinction between objective and perceived risk. Users balance technical recommendations against convenience, cognitive effort, and perceived benefits [17]. Memory anxiety can affect password behaviour [18], while adaptive and maladaptive mechanisms influence password-manager adoption [19]. Recent evidence also questions whether unique passwords necessarily impose greater memorability costs than reused or modified passwords [20]. Security behaviour should therefore be understood as the outcome of a decision process in which objective technological risks are interpreted before being translated into protective action, risky behaviour, or inaction.

2.3 Trust, Reliability, and Emerging Technological Contexts

Trust is another central mechanism linking technological risk with behaviour. Because users cannot fully evaluate the internal operation and vulnerabilities of complex digital systems, some degree of reliance is unavoidable. However, excessive trust may increase inappropriate reliance; cybersecurity therefore requires calibrated trust rather than simply greater trust. This relationship is particularly visible in connected and autonomous technologies. Trust and perceived risk

influence autonomous-vehicle adoption [21], cybersecurity attacks can reduce trust in automated operation [22], and cyber readiness and system responses affect both trust and blame attribution [23]. Trust also operates at the organisational level, where interpersonal and institutional relationships can influence safety and security [24]. In critical infrastructures, these human factors become particularly important because failures may affect organisational continuity and broader societal functions [25], [26]. Similar socio-technical interactions occur in BYOD environments, where organisational policies, device ownership, user preferences, and security behaviour interact [27], [28], encouraging more integrated security-management approaches [29]. Emerging technologies extend these challenges: quantum computing may threaten established encryption mechanisms [30], while AI-supported environments raise new questions concerning security governance and trust calibration [31]. Across these contexts, a common structure emerges: technological conditions create vulnerabilities, users and organisations interpret these risks, and trust and perceived control influence subsequent responses. Technological risk, risk perception, trust, organisational context, and security behaviour can therefore be treated as interconnected components of a broader human-centred cybersecurity process.

3 Research Questions

Based on the conceptual background and the identified fragmentation between technological and human-centred approaches to cybersecurity, the review addresses the following research questions:

RQ1. *What human factors are most frequently associated with secure and insecure information-security behaviour?*

RQ2. *How do risk perception, perceived vulnerability, and trust influence security-related decision-making and behaviour?*

RQ3. *How are technological risks, system failures, and reliability issues connected to human responses and security outcomes?*

RQ4. *To what extent do common human and organisational mechanisms emerge across different technological contexts, including mobile technologies, IoT, BYOD, autonomous systems, and critical infrastructures?*

4 Methodology

4.1 Review Design

This study adopts a systematic literature review design to identify and synthesise recent research on human factors, information security, and technological risk. The review was structured according to the reporting principles of PRISMA 2020 [32]. The systematic corpus was restricted to studies published between 2020 and 2026, while earlier publications were used only as background references. The final literature search was conducted on August 19, 2026; consequently, publications from 2026 represent studies available up to the search cut-off date.

4.2 Search Strategy

The primary search covered Scopus and Web of Science, complemented by IEEE Xplore, ScienceDirect, and SpringerLink. Searches targeted titles, abstracts, and keywords using combinations of cybersecurity, technological-risk, and human-factor terms. The core search string was:

“cybersecurity” OR “information security” OR “cyber risk” OR “security risk” OR “technological risk”) AND (“human factor*” OR “human behaviour” OR “human behavior” OR “user behaviour” OR “user behavior” OR “security behaviour” OR “security behavior” OR “risk perception” OR “perceived vulnerability” OR “trust” OR “decision making” OR “decision-making” OR “perceived control”)

Additional searches targeted the technological contexts represented in the review:

“cybersecurity” OR “information security” OR “technological risk”) AND (“BYOD” OR “Internet of Things” OR “IoT” OR “mobile device*” OR “smartphone*” OR “autonomous vehicle*” OR “automated vehicle*” OR “critical infrastructure*” OR “quantum computing”)

Search syntax was adapted to individual databases where necessary.

Additional eligible publications identified through supplementary author- and reference-based searches were assessed using the same inclusion and exclusion criteria and incorporated into the final corpus.

4.3 Eligibility and Study Selection

Studies were eligible if they (1) were published between 2020 and 2026; (2) were peer-reviewed journal articles, review articles, or scholarly book chapters/proceedings contributions; (3) addressed cybersecurity, information security, technological risk, or system reliability; (4) explicitly considered a human or organisational dimension, such as behaviour, risk perception, trust, awareness, decision-making, compliance, or perceived control; and (5) provided sufficient

methodological or conceptual detail for thematic analysis. Publications in English and Hungarian were considered. Studies focusing exclusively on technical mechanisms, general technology adoption without a meaningful security or risk component, non-scholarly material, and duplicate records were excluded. Study selection followed four stages consistent with PRISMA 2020: identification, screening, eligibility assessment, and inclusion [32]. After duplicate removal, titles and abstracts were screened against the eligibility criteria, followed by full-text assessment. The final systematic corpus comprised 47 publications. Methodological and pre-2020 background sources were not included in the systematic corpus.

4.4 Data Extraction and Thematic Synthesis

For each publication, information was extracted on publication year, technological or organisational context, research design, principal human or organisational constructs, technological-risk dimension, and findings relevant to the research questions. The corpus included quantitative and qualitative studies, systematic reviews, conceptual contributions, and selected scholarly book chapters and conference contributions.

The studies were compared iteratively and organised into five recurring themes:

- Human factors and security behaviour
- Risk perception and security-related decision-making
- Trust and organisational security
- Technological risk, system failure, and reliability
- Critical infrastructures and emerging technologies

Studies could contribute to more than one theme; the categories were therefore treated as interconnected rather than mutually exclusive. The cross-thematic synthesis was subsequently used to develop the Integrated Human-Centred Cybersecurity Risk Framework presented in the Discussion.

5 Results and Thematic Synthesis

The review identified five interconnected domains: (1) human factors and security behaviour, (2) risk perception and security-related decision-making, (3) trust and organisational security, (4) technological risk, system failure, and reliability, and (5) critical infrastructures and emerging technologies. These themes overlap substantially, particularly through risk perception, trust, and decision-making, which connect technological conditions with behavioural and organisational security outcomes. Together, these five themes address the four research questions by covering individual and organisational determinants of security behaviour

(RQ1), risk perception and trust (RQ2), technological risk and reliability (RQ3), and recurring mechanisms across technological contexts (RQ4).

Theme	Main constructs	Main analytical focus
Human factors and security behaviour	Awareness, knowledge, human error, compliance, self-efficacy, motivation	Determinants of secure and insecure behaviour
Risk perception and decision-making	Perceived vulnerability, severity, risk propensity, benefits, coping appraisal	Interpretation of threats and behavioural responses
Trust and organisational security	Technological and organisational trust, perceived control, security culture	Role of trust and organisational context
Technological risk and reliability	Failure, vulnerability, reliability, FMEA, technical risk	Objective technological risk and human response
Critical infrastructures and emerging technologies	IoT, BYOD, autonomous systems, critical infrastructure, quantum computing, AI	Human-technology interaction in evolving environments

Table 1.
Thematic structure of the reviewed literature

5.1 Human Factors and Security Behaviour

Human factors emerged as a consistent determinant of cybersecurity outcomes. Knowledge and personal characteristics are associated with security practices [12], while insecure behaviour may result from passive inaction rather than deliberate risk-taking [13]. Organisational and information-security cultures further influence compliance [8], confirming that security behaviour is embedded within broader socio-technical environments [2]–[4]. Motivational mechanisms are similarly diverse. Protection motivation interacts with stewardship [33], while intrinsic and identity-based motivations [34], as well as prosocial, self-regulatory, and deterrence-related mechanisms [16], can also contribute to security behaviour. BYOD research reinforces the contextual nature of these relationships: individual preferences, organisational policies, compliance requirements, knowledge, and everyday working practices jointly shape security behaviour [27], [28], [35], [11]. Human factors can therefore represent both sources of vulnerability and components of security resilience [9]. The broader ICT environment of SMEs further demonstrates that organisational technology use and innovation practices form an important contextual layer within which security-related behaviour takes place [47].

5.2 Risk Perception and Security-Related Decision-Making

The reviewed studies distinguish technological vulnerability from its subjective interpretation. Perceived vulnerability [14], cognitive and motivational mechanisms [15], knowledge [12], and passive-risk tendencies [13] influence whether users respond protectively to cybersecurity threats. Password management illustrates this relationship particularly clearly. Users balance security requirements against perceived risks, benefits, convenience, and cognitive effort [17]. Memory anxiety affects password-security decisions [18], adaptive and maladaptive factors influence password-manager use [19], and recent findings challenge assumptions concerning the memorability costs of unique passwords [20]. Additional password-security research similarly highlights the continuing importance of user-side practices in determining the effectiveness of technical protection [36]. Comparable decision processes occur in smartphone and BYOD environments [27], [28], [37]. These findings support a central distinction between objective technological risk and subjective risk perception: technical vulnerability creates the possibility of harm, while subjective appraisal influences whether users adopt, postpone, circumvent, or reject protective measures.

5.3 Trust and Organisational Security

Trust connects technological conditions with human responses but is not uniformly beneficial. At the organisational level, security culture and trust shape employee behaviour and relationships among users, technologies, and institutions [8], [24], while BYOD governance requires organisations to balance control, autonomy, and technological risk [10]. This relationship is particularly visible in autonomous systems. Trust and perceived risk influence technology adoption [21]; cybersecurity attacks can substantially reduce trust [22]; and cyber readiness and response affect trust and blame attribution [23]. Readiness and societal perceptions of autonomous vehicles further demonstrate that technological capability alone does not determine preparedness or acceptance [38], [39]. Recent human-centred research also differentiates driver responses to cyber-attacks in automated vehicles, further demonstrating that cybersecurity incidents can produce heterogeneous behavioural responses [40].

5.4 Technological Risk, System Failure, and Reliability

Engineering-oriented studies provide an objective-risk perspective by identifying technological failures and vulnerabilities. FMEA-based smartphone analysis demonstrates how failures can be systematically prioritised [5], while mobile-device research identifies hardware and software factors affecting reliability [41]. Human-centred research complements this perspective by examining whether users recognise these risks and respond appropriately. Password security illustrates how

technically stronger practices may conflict with cognitive or practical considerations [17]–[20], [36], while mobile and BYOD environments require security measures to coexist with usability and everyday organisational practices [27]–[29]. The same relationship extends to cyber-physical systems. Connected and autonomous vehicle research integrates technological, human, and contextual cybersecurity dimensions [7], while expert evidence identifies cybersecurity and privacy as significant concerns [42]. Thus, technological reliability and human behaviour represent complementary dimensions of security risk rather than independent problems. Blockchain-based solutions provide a complementary technological perspective, illustrating how decentralised and cryptographically protected data storage can be incorporated into security-sensitive digital systems [48].

5.5 Critical Infrastructures and Emerging Technologies

Critical infrastructures make the interaction between technological and human risk particularly consequential. Human factors can contribute to both vulnerability and resilience [25], and security-management research demonstrates the importance of incorporating users and operators into interconnected critical-infrastructure protection [26]. Comparable socio-technical challenges arise in IoT and BYOD environments, where interconnectivity and organisational boundaries increase the importance of integrated technological, behavioural, and governance approaches [3], [29]. Cross-context comparisons between BYOD and autonomous vehicles further suggest that similar user-related cybersecurity challenges can recur across otherwise distinct technological environments [43]. Autonomous systems similarly combine cybersecurity, privacy, trust, readiness, and institutional concerns [7], [21], [22], [38], [42], [39], with military applications adding further safety and security considerations [44]. Emerging technologies extend these challenges. Quantum computing may undermine established encryption mechanisms [30], while AI-supported environments introduce new requirements for governance and trust calibration [31]. Across these contexts, increasing technological complexity simultaneously creates new vulnerabilities and greater dependence on systems that users and organisations cannot fully evaluate. Blockchain-based applications further illustrate how emerging digital architectures can reshape data management, verification, and security requirements across organisational environments [49].

5.6 Cross-Thematic Synthesis

Across the five themes, technological conditions, risk perception, trust, perceived control, decision-making, and security behaviour emerged as recurrent and interconnected dimensions. Individual factors—including knowledge, awareness, experience, self-efficacy, motivation, and risk tendencies—shape how threats are interpreted [12]–[20], [33], [34], while organisational factors such as security

culture, policies, management practices, trust, and governance influence the decision environment [8], [10], [24]–[29]. Security outcomes can, in turn, affect subsequent perceptions and behaviour. Cybersecurity incidents and technological failures may modify risk perception and trust [22], [23], while research on behavioural responses to attacks further indicates that these effects need not be uniform across users or situations [40]. These cross-thematic relationships provide the basis for the Integrated Human-Centred Cybersecurity Risk Framework developed in the Discussion.

6 Discussion

The findings indicate that cybersecurity cannot be adequately explained from either a purely technical or behavioural perspective. Across the reviewed contexts, technological conditions acquire behavioural relevance through risk perception, trust, perceived control, and decision-making. The main contribution of the synthesis is therefore to integrate these mechanisms within a common socio-technical process.

6.1 From Technological Risk to Human Behaviour

Security behaviour reflects a combination of individual and organisational mechanisms. Knowledge and personal characteristics influence security practices [12], while insecure outcomes may result from passive inaction rather than deliberate risk-taking [13]. Motivation [33], [34] and organisational security culture [8] further shape behavioural responses. These findings challenge the conventional characterisation of users simply as the “weakest link.” Human involvement can generate vulnerability but also provide adaptability, threat recognition, judgement, and resilience [2], [9]. Security interventions should therefore address not only knowledge but also users’ capabilities, motivation, perceived relevance of threats, and organisational environment. The findings also reinforce the distinction between objective technological risk and subjective risk perception. Technical methods identify vulnerabilities and failures [5], [41], whereas behavioural responses depend on how these risks are interpreted [14]–[20]. The two dimensions are therefore complementary: technological risk defines the underlying conditions, while risk perception determines their behavioural relevance. Cybersecurity management should consequently seek risk calibration rather than risk maximisation, as both underestimation and excessive perceived risk may produce undesirable responses.

6.2 Trust and Technological Context

Trust should similarly be calibrated rather than maximised. Excessive trust can encourage inappropriate reliance, while insufficient trust can inhibit or distort technology use. Autonomous-system research illustrates this clearly: trust and perceived risk affect adoption [21], cybersecurity incidents can produce persistent reductions in trust [22], and cyber readiness and response influence both trust and blame [23]. Human responses to cyber-attacks may also vary substantially across users and situations [40]. Organisational trust extends this mechanism beyond direct human–technology interaction [24]. Although these mechanisms recur across technological contexts, their consequences vary. Passwords, mobile devices, BYOD, IoT, autonomous vehicles, and critical infrastructures differ substantially in complexity and potential impact [3], [7], [25], [27], [38], [42]. Cross-context comparisons between BYOD and autonomous vehicles nevertheless indicate recurring user-related cybersecurity challenges [43]. The evidence therefore suggests that risk perception, trust, perceived control, and decision-making may represent transferable mechanisms, while the magnitude and consequences of risk remain technology-specific.

6.3 Integrated Human-Centred Cybersecurity Risk Framework

Based on the cross-thematic synthesis, this review proposes an Integrated Human-Centred Cybersecurity Risk Framework linking technical, cognitive, behavioural, and organisational dimensions: Technological and contextual conditions include vulnerabilities, reliability, attack exposure, complexity, and the operational environment. These conditions are interpreted through threat appraisal and subsequently influence trust, perceived control, decision-making, and security behaviour, including protective action, circumvention, or inaction [13]. As summarised in Figure 1, the process is shaped by cross-cutting individual, organisational, and technological factors. It is also recursive rather than strictly linear: security incidents, system failures, protective actions, and organisational responses can modify subsequent risk perception and trust, creating feedback into future decisions and behaviour [22], [23]. The framework represents a conceptual synthesis rather than a statistically validated causal model. Its purpose is to integrate relationships that are often examined separately and provide a structure for future empirical testing.

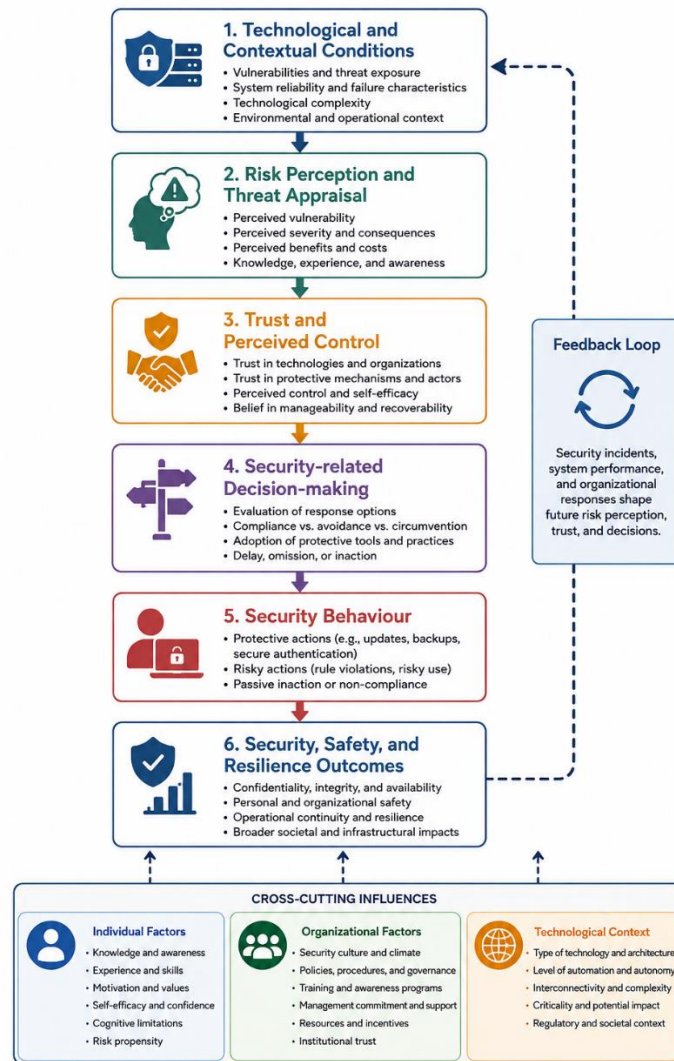


Figure 1.
Integrated Human-Centred Cybersecurity Risk Framework

6.4 Theoretical and Practical Implications

The principal theoretical contribution is the integration of technical risk assessment with behavioural and organisational explanations of cybersecurity outcomes. This

perspective distinguishes objective technological conditions from their subjective interpretation while incorporating calibrated trust as a mechanism connecting risk appraisal with behaviour. These relationships are particularly relevant in autonomous, AI-supported, and critical systems [31].

For practice, security management should combine technical controls with behavioural and organisational interventions. Awareness and training should be complemented by attention to perceived vulnerability, self-efficacy, usability, cognitive burden, organisational culture, and the practical costs of compliance. BYOD research demonstrates how security measures that conflict with everyday practices may encourage circumvention [27]–[29], [35]. Risk communication should likewise seek to align perceived and objective risk while providing understandable and feasible protective responses. As systems become increasingly interconnected and autonomous—including developments associated with quantum computing and AI [30], [31]—human-centred risk management should be treated as an integral component of cybersecurity strategy. More broadly, differences in organisational digital transformation may shape the technological and managerial context in which cybersecurity practices and risk-management measures are implemented [46].

7 Limitations and Future Research

This review has several limitations. First, the systematic corpus was restricted to studies published between 2020 and 2026, with the 2026 coverage limited to publications available by the final search date; earlier contributions were used only selectively as background literature. Second, the reviewed studies are heterogeneous in technological context, research design, theoretical perspective, and measurement of constructs such as risk perception, trust, and security behaviour. This supports cross-context conceptual synthesis but limits direct quantitative comparison and meta-analytic interpretation. Finally, the five thematic categories are interconnected rather than mutually exclusive and should therefore be interpreted as a synthesis framework rather than a rigid taxonomy. Future research should examine objective technological risk and subjective risk perception simultaneously, particularly whether discrepancies between them influence security behaviour. Longitudinal and experimental studies are also needed to investigate how security incidents alter trust and how trust is subsequently restored or recalibrated [22], [23]. Comparative research across technological contexts could further establish which relationships among risk perception, trust, perceived control, and security behaviour are generalisable and which remain technology-specific. Finally, the Integrated Human-Centred Cybersecurity Risk Framework proposed here requires empirical validation. Future studies could operationalise its

components and test their relationships using structural models, experiments, longitudinal designs, or mixed-method approaches.

Conclusion

This systematic literature review synthesised 47 publications from 2020 to 2026 to examine the relationship between human factors, information security, and technological risk. The findings demonstrate that cybersecurity is inherently socio-technical: technological vulnerabilities acquire behavioural relevance through risk perception, trust, perceived control, decision-making, and organisational conditions. A central conclusion is that objective technological risk and subjective risk perception should be distinguished but analysed jointly. Technical vulnerability alone does not determine security behaviour, while perceived risk depends on how technological conditions are interpreted. Similarly, effective cybersecurity requires calibrated rather than maximised trust, aligning users' confidence with actual system capabilities, vulnerabilities, and safeguards. Based on these relationships, the study proposes an Integrated Human-Centred Cybersecurity Risk Framework that integrates technological, cognitive, behavioural, and organisational dimensions of cybersecurity within a recursive socio-technical process. The framework provides a basis for examining how technological conditions are translated into security behaviour and outcomes across different technological contexts. Overall, human factors should not be treated merely as vulnerabilities within otherwise technical systems. Human judgement, knowledge, adaptation, and organisational behaviour are integral components of cybersecurity. As digital systems become increasingly interconnected and autonomous, effective security will require the integration of technical reliability, human behaviour, calibrated trust, and organisational resilience.

References

- [1] R. A. Alsharida, B. A. S. Al-rimy, M. Al-Emran, and A. Zainal, "A systematic review of multi perspectives on human cybersecurity behavior," *Technology in Society*, vol. 73, Art. no. 102258, 2023, <https://doi.org/10.1016/j.techsoc.2023.102258>.
- [2] A. Pollini, T. C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, and D. Guerri, "Leveraging human factors in cybersecurity: An integrated methodological approach," *Cognition, Technology & Work*, vol. 24, pp. 371–390, 2022, <https://doi.org/10.1007/s10111-021-00683-y>.
- [3] K. Hughes-Lartey, M. Li, and F. E. Botchey, "Human factor, a critical weak point in the information security of an organization's Internet of Things," *Heliyon*, vol. 7, no. 3, Art. no. e06522, 2021, <https://doi.org/10.1016/j.heliyon.2021.e06522>.

- [4] S. Nifakos, K. Chandramouli, C. K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis, and S. Bonacina, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, Art. no. 5119, 2021, <https://doi.org/10.3390/s21155119>.
- [5] E. Kadena, S. Koçak, K. Takács-György, and A. Keszthelyi, "FMEA in smartphones: A fuzzy approach," *Mathematics*, vol. 10, no. 3, Art. no. 513, 2022, <https://doi.org/10.3390/math10030513>.
- [6] T. Schaltegger, B. Ambuehl, N. Bosshart, A. Bearth, and N. Ebert, "Human behavior in cybersecurity: An opportunity for risk research," *Journal of Risk Research*, vol. 28, no. 8, pp. 843–854, 2025, <https://doi.org/10.1080/13669877.2025.2539109>.
- [7] S. K. Khan, N. Shiwakoti, and P. Stasinopoulos, "A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles," *Accident Analysis & Prevention*, vol. 165, Art. no. 106515, 2022, <https://doi.org/10.1016/j.aap.2021.106515>.
- [8] G. Solomon and I. Brown, "The influence of organisational culture and information security culture on employee compliance behaviour," *Journal of Enterprise Information Management*, vol. 34, no. 4, pp. 1203–1228, 2021, <https://doi.org/10.1108/JEIM-08-2019-0217>.
- [9] S. Colabianchi, F. Costantino, F. Nonino, and G. Palombi, "Transforming threats into opportunities: The role of human factors in enhancing cybersecurity," *Journal of Innovation & Knowledge*, vol. 10, no. 3, Art. no. 100695, 2025, <https://doi.org/10.1016/j.jik.2025.100695>.
- [10] Y. Barlette, A. Jaouen, and P. Baillelte, "Bring your own device (BYOD) as reversed IT adoption: Insights into managers' coping strategies," *International Journal of Information Management*, vol. 56, Art. no. 102212, 2021, <https://doi.org/10.1016/j.ijinfomgt.2020.102212>.
- [11] R. Palanisamy, S. Norman, and M. Kiah, "Compliance with bring your own device security policies in organizations: A systematic literature review," *Computers & Security*, vol. 98, Art. no. 101998, 2020, <https://doi.org/10.1016/j.cose.2020.101998>.
- [12] S. M. Kennison and E. Chan-Tin, "Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors," *Frontiers in Psychology*, vol. 11, Art. no. 546546, 2020, <https://doi.org/10.3389/fpsyg.2020.546546>.
- [13] I. Arend, A. Shabtai, T. Idan, R. Keinan, and Y. Bereby-Meyer, "Passive- and not active-risk tendencies predict cyber security behavior," *Computers & Security*, vol. 97, Art. no. 101964, 2020, <https://doi.org/10.1016/j.cose.2020.101964>.

- [14] S. M. Debb and M. K. McClellan, "Perceived vulnerability as a determinant of increased risk for cybersecurity risk behavior," *Cyberpsychology, Behavior, and Social Networking*, vol. 24, no. 9, pp. 605–611, 2021, <https://doi.org/10.1089/cyber.2021.0043>.
- [15] L. Li, L. Xu, and W. He, "The effects of antecedents and mediating factors on cybersecurity protection behavior," *Computers in Human Behavior Reports*, vol. 5, Art. no. 100165, 2022, <https://doi.org/10.1016/j.chbr.2021.100165>.
- [16] Y. Chen, W. Xia, and K. Cousins, "Voluntary and instrumental information security policy compliance: An integrated view of prosocial motivation, self-regulation and deterrence," *Computers & Security*, vol. 113, Art. no. 102568, 2022, <https://doi.org/10.1016/j.cose.2021.102568>.
- [17] B. Merdenyan and H. Petrie, "Two studies of the perceptions of risk, benefits and likelihood of undertaking password management behaviours," *Behaviour & Information Technology*, vol. 41, no. 12, pp. 2514–2527, 2022, <https://doi.org/10.1080/0144929X.2021.2019832>.
- [18] N. Woods and M. Siponen, "How memory anxiety can influence password security behavior," *Computers & Security*, vol. 137, Art. no. 103589, 2024, <https://doi.org/10.1016/j.cose.2023.103589>.
- [19] A. Nehme, M. Li, and M. Warkentin, "Adaptive and maladaptive factors behind password manager use: A hope-extended protection motivation perspective," *Computers & Security*, vol. 144, Art. no. 103941, 2024, <https://doi.org/10.1016/j.cose.2024.103941>.
- [20] N. Woods and M. Siponen, "Questioning a security assumption: Are unique passwords harder to remember than reused or modified passwords?" *Computers & Security*, vol. 157, Art. no. 104545, 2025, <https://doi.org/10.1016/j.cose.2025.104545>.
- [21] Z. Kenesei, K. Ásványi, L. Kökény, M. Jászberényi, M. Miskolczi, T. Gyulavári, and J. Syahrivar, "Trust and perceived risk: How different manifestations affect the adoption of autonomous vehicles," *Transportation Research Part A: Policy and Practice*, vol. 164, pp. 379–393, Oct. 2022, doi: <https://doi.org/10.1016/j.tra.2022.08.022>.
- [22] C. Lim, D. Prendez, L. N. Boyle, and P. Rajivan, "The impact of cybersecurity attacks on human trust in autonomous vehicle operations," *Human Factors*, vol. 67, no. 5, pp. 485–502, 2025, <https://doi.org/10.1177/00187208241283321>.
- [23] V. Marcinkiewicz, Q. Zhang, M. Asada, Y. Ueda, H. Katsuno, T. Inatani, and P. L. Morgan, "Trust and blame in autonomous vehicles: Examining the effects of cyber readiness and response in the UK and Japan," *Transportation*

Research Part F: Traffic Psychology and Behaviour, vol. 119, Art. no. 103589, 2026, <https://doi.org/10.1016/j.trf.2026.103589>.

- [24] K. Lazányi and A. Danaj, “Can trust be a factor of organisational safety and security?” in *Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach*, T. A. Kovács, Z. Nyikes, and I. Fürstner, Eds. Springer, 2022, pp. 379–390, https://doi.org/10.1007/978-94-024-2174-3_33.
- [25] K. Lazányi and A. Danaj, “Critical threat of critical infrastructures: The human factor,” in *Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach*, T. A. Kovács, Z. Nyikes, and I. Fürstner, Eds. Springer, 2022, pp. 1–11, https://doi.org/10.1007/978-94-024-2174-3_1.
- [26] F. Pickert, T. H. Stelkens-Kobsch, M. Schaper, H. Boumann, and N. Carstengerdes, “A human factor-centric validation of a security management system in a linked critical infrastructure environment,” *Human-Intelligent Systems Integration*, vol. 7, pp. 341–359, 2025, <https://doi.org/10.1007/s42454-025-00070-2>.
- [27] K. Downer and M. Bhattacharya, “BYOD security: A study of human dimensions,” *Informatics*, vol. 9, no. 1, Art. no. 16, 2022, <https://doi.org/10.3390/informatics9010016>.
- [28] T. A. Wani, A. Mendoza, K. Gray, and F. Smolenaers, “BYOD usage and security behaviour of hospital clinical staff: An Australian survey,” *International Journal of Medical Informatics*, vol. 165, Art. no. 104839, 2022, <https://doi.org/10.1016/j.ijmedinf.2022.104839>.
- [29] T. A. Wani, A. Mendoza, and K. Gray, “A sociotechnical approach to bring-your-own-device security in hospitals: Development and pilot testing of a maturity model using mixed methods action research,” *JMIR Human Factors*, vol. 12, Art. no. e71912, 2025, <https://doi.org/10.2196/71912>.
- [30] P. Szikora and K. Lazányi, “The end of encryption?—The era of quantum computers,” in *Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach*, T. A. Kovács, Z. Nyikes, and I. Fürstner, Eds. Springer, 2022, pp. 61–72, https://doi.org/10.1007/978-94-024-2174-3_5.
- [31] J. Żywiołek, R. Wolniak, and W. W. Grebski, “Embedding governance in AI security culture: From trust calibration to accountable decisions,” *International Journal of Information Security*, vol. 25, Art. no. 95, 2026, <https://doi.org/10.1007/s10207-026-01265-7>.
- [32] M. J. Page et al., “The PRISMA 2020 statement: An updated guideline for reporting systematic reviews,” *BMJ*, vol. 372, Art. no. n71, 2021, <https://doi.org/10.1136/bmj.n71>.

- [33] O. Ogbanufe, R. E. Crossler, and D. P. Biros, "The valued coexistence of protection motivation and stewardship in information security behaviors," *Computers & Security*, vol. 124, Art. no. 102960, 2023, <https://doi.org/10.1016/j.cose.2022.102960>.
- [34] O. Ogbanufe and L. Ge, "A comparative evaluation of behavioral security motives: Protection, intrinsic, and identity motivations," *Computers & Security*, vol. 128, Art. no. 103136, 2023, <https://doi.org/10.1016/j.cose.2023.103136>.
- [35] T. A. Wani, A. Mendoza, and K. Gray, "BYOD security behaviour and preferences among hospital clinicians: A qualitative study," *International Journal of Medical Informatics*, vol. 192, Art. no. 105606, 2024, <https://doi.org/10.1016/j.ijmedinf.2024.105606>.
- [36] A. Keszthelyi, "A jelszó lehet jó is meg ham is," *Taylor*, vol. 15, no. 1, pp. 9–18, 2025.
- [37] N. Ameen, A. Tarhini, M. H. Shah, and N. O. Madichie, "Employees' behavioural intention to smartphone security: A gender-based, cross-national study," *Computers in Human Behavior*, vol. 104, Art. no. 106184, 2020, <https://doi.org/10.1016/j.chb.2019.106184>.
- [38] P. Szikora and R. Szatmáry, "Autonomous cars—What lies behind the lack of readiness," *Interdisciplinary Description of Complex Systems*, vol. 21, no. 4, pp. 399–411, 2023, <https://doi.org/10.7906/indexcs.21.4.9>.
- [39] P. Szikora, "Autonomous travel: Changes in driving and its perception in society," *Vezetéstudomány / Budapest Management Review*, vol. 56, no. 3, pp. 55–64, 2025, <https://doi.org/10.14267/VEZTUD.2025.03.05>.
- [40] G. Ban, K. Zhang, U. Mudgil, and M. Jeon, "A human-centered taxonomy of driver responses to cyber-attacks in automated vehicles," *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 119, Art. no. 103595, 2026, <https://doi.org/10.1016/j.trf.2026.103595>.
- [41] E. Kadena and A. Keszthelyi, "Identifying failures in mobile devices," *Interdisciplinary Description of Complex Systems*, vol. 20, no. 3, pp. 222–229, 2022, <https://doi.org/10.7906/indexcs.20.3.1>.
- [42] N. Liu, A. Nikitas, and S. Parkinson, "Exploring expert perceptions about the cyber security and privacy of connected and autonomous vehicles: A thematic analysis approach," *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 75, pp. 66–86, 2020, <https://doi.org/10.1016/j.trf.2020.09.019>.
- [43] P. Michelberger and P. Fehér-Polgár, "BYOD security strategy (aspects of a managerial decision)," *Journal of Security and Sustainability Issues*, vol. 9, no. 4, pp. 1135–1143, Jun. 2020, [https://doi.org/10.9770/jssi.2020.9.4\(1\)](https://doi.org/10.9770/jssi.2020.9.4(1)).

- [44] P. Szikora, "Who can support the introduction of self-driving military vehicles?" *Honvédségi Szemle*, vol. 153, no. SI1, pp. 67–79, Jun. 2025, <https://doi.org/10.35926/HDR.2025.1.6>.
- [45] B. Ali and P. Szikora, "Információbiztonság az Y generáció körében," in *Vállalkozásfejlesztés a XXI. században VII.*, Á. Csiszárík-Kocsir, Ed. Budapest, Hungary: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2017, pp. 24–40.
- [46] A. B. Horváth, "Different approach of the digital transformation at SME," *Acta Polytechnica Hungarica*, vol. 20, no. 9, pp. 145–164, 2023, <https://doi.org/10.12700/APH.20.9.2023.9.9>.
- [47] A. B. Horváth, "Research on ICT innovation in Hungarian SMEs," *Business and IT*, vol. 13, no. 1, pp. 203–212, 2023, <https://doi.org/10.14311/bit.2023.01.22>.
- [48] K. Bálint, "Possibilities for the utilization of an automatized, electronic blockchain-based, students' attendance register, using a universities' modern security cameras," *Acta Polytechnica Hungarica*, vol. 18, no. 2, pp. 127–142, 2021, <https://doi.org/10.12700/APH.18.2.2021.2.7>.
- [49] K. Bálint, "Blockchain technology supported education," in *2024 9th International Conference on Smart and Sustainable Technologies (SpliTech)*, 2024, <https://doi.org/10.23919/SpliTech61897.2024.10612401>.