



OPEN ACCESS

EDITED BY

Saqib Saeed,
Imam Abdulrahman Bin Faisal University,
Saudi Arabia

REVIEWED BY

Hewa Majeed Zangana,
University of Duhok, Iraq
Prasetyo Adi Wibowo Putro,
Politeknik Siber dan Sandi Negara,
Indonesia

*CORRESPONDENCE

Ravdeep Kour
✉ ravdeep.kour@ltu.se

RECEIVED 10 December 2025
REVISED 05 February 2026
ACCEPTED 11 February 2026
PUBLISHED 26 February 2026

CITATION

Kour R, Karim R and
Wägenbauer A (2026) Annoyed by
cybersecurity? Human-centric
perspectives on cybersecurity.
Front. Comput. Sci. 8:1764808.
doi: 10.3389/fcomp.2026.1764808

COPYRIGHT

© 2026 Kour, Karim and Wägenbauer.
This is an open-access article distributed
under the terms of the [Creative
Commons Attribution License \(CC BY\)](#).
The use, distribution or reproduction in
other forums is permitted, provided the
original author(s) and the copyright
owner(s) are credited and that the
original publication in this journal is
cited, in accordance with accepted
academic practice. No use, distribution
or reproduction is permitted which does
not comply with these terms.

Annoyed by cybersecurity? Human-centric perspectives on cybersecurity

Ravdeep Kour^{1*}, Ramin Karim¹ and Annika Wägenbauer²

¹Division of Operation and Maintenance Engineering, Lulea University of Technology, Luleå, Sweden,
²Cybersecurity Redefined, Stuttgart, Germany

Humans play a vital role in designing, developing, implementing, and using technical systems. For this reason, it is crucial to keep humans in the loop at each phase of these systems to make them more secure and user-friendly. There needs to be a balance between using these systems securely and making them easy to use. Today, under pressure to secure our systems from cyberattacks, we primarily focus on making them secure but often overlook making them easy to use. Thus, the objective of this paper is to provide a human-centric perspective on cybersecurity and to introduce a human-centric framework that enables Industry 5.0, where humans have direct interaction with systems and solutions that are more customer-oriented. To carry out this research, the authors have applied the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to investigate human-centric research over a 10-year period, from 2015 to 2025. The literature shows that most human-centric research contributions are well-balanced, with conceptual, experimental, and survey approaches each accounting for approximately 64% of the total, indicating a mature blend of theoretical and applied research. These studies are focused on developing structured, strategic approaches that integrate human factors into cybersecurity practices across sectors such as education, government, health, software, smart home networks, and others. To conduct this research, the authors have prepared an anonymous questionnaire with fundamental questions about secure system's design, which can be easily used. The evaluation results show that frequent password resets (33.3%) and frequent authentication (26.7%) are the most "annoying" cybersecurity measures. Additionally, most respondents consider biometric login the most user-friendly security feature, followed by single sign-on and automatic security patch updates. What is missing in existing literature and studies is a holistic perspective on human-centrism, beyond mere ease of use. We aim to cover that blind spot by introducing our independently developed framework in this paper.

KEYWORDS

annoyance, cybersecurity, framework, human-centric, review

1 Introduction

Cybersecurity plays a crucial role in the digital era. Sometimes, it seems that excessive cybersecurity is a hindrance to end users. Instead of following cybersecurity measures because of their annoyance, users opt for easy alternatives that can lead to system vulnerabilities. Based on a survey, the most reflected annoyances related to cybersecurity were frequent password changes (21.6%) and multiple authentication steps (Hadi, 2023). This leads to a high cognitive

cost, which refers to the mental effort users put in while dealing with security measures that can lead to security fatigue and mistakes (Hadi, 2023). Additionally, researchers have mentioned some of the factors that many employees fail to follow, such as inconvenience (MFA, complex password requirements, or software updates), lack of awareness (clicking on a malicious link or weak password), and complacency and overconfidence (Ayodele et al., 2025).

Thus, we must strike a balance between providing cyber-secure systems and their ease of usability. This usability factor can be incorporated when we think from the perspective of end users, and we need to understand their psychology. The literature reveals a lack of empirical research on the use of psychology in cybersecurity. To address this, we need to consider humans as a central part of cybersecurity, moving toward a human-centric perspective rather than a technology-centric one (Hakimi et al., 2024).

Researchers are talking about the current systems where security is added at the expense of usability, and there is a need for a balance between cybersecurity and usability (van der Kleij et al., 2024). Some of the researchers have proposed human-centric cybersecurity by integrating user, usage, and usability (the 3Us) into security design, implementation, and deployment (Grobler et al., 2021). Other researchers are considering user, system, and usability as the three pillars of cybersecurity from a Computer Science community perspective (Rahman et al., 2021). They have explored human-centric cybersecurity (HC-CS), considering not only technical users such as software developers, security professionals, and code testers, but also regular users who use the system (Rahman et al., 2021). There is no standard definition of HC-CS in the literature, and the term is used somewhat vaguely. Table 1 summarises definitions of HC-CS found in the literature. Most researchers observe that HC-CS is inherently difficult to define due to the complex interconnections among humans, technology, and security systems.

1.1 Human-centric cybersecurity and people, process, and technology framework

The concepts used in the definitions provided in Table 1 resemble a popular framework called People, Process, and Technology (PPT), introduced by Leavitt (1964) and restructured by Schneier (2015) in the context of IT security, as presented in Figure 1. Each element of the PPT framework is briefly discussed:

- Technologies provide essential security measures, including firewalls, encryption, biometrics, password protection, and intrusion detection.
- Processes such as risk assessments, incident response, vulnerability management, identity and authentication management, and access control management ensure effective management and control.
- Both technologies and processes depend on people, including administrators, managers, software developers, security professionals, code testers, and end-users, whose training and awareness are critical to make them the “strongest link” from the “weakest link” referred to in most of the literature.

Thus, to redefine human-centric cybersecurity in the context of the PPT framework is:

“An approach that integrates people, processes, and technology by prioritising usability and human behaviour, ensuring humans are

skilled and informed, processes are clear and adaptable, and technologies support real human needs, creating resilient and sustainable security.”

This definition also aligns with the context of Industry 5.0, “Toward a Sustainable, Human-centric, and Resilient European Industry,” encouraging industries to reassess their positions and roles in society (Breque et al., 2021). In order to attain this position and role in society, we need trained and well-aware humans on both sides (developers of the system and users of the system). Thus, making a need for a well-defined training program that is both human-centric and user-friendly. Such training initiatives have been implemented by regional universities, where 82% of over 2,000 employees completed the program, with more than half of the units achieving 100% completion, and 91% of faculty participating (Coffey et al., 2018). We need such initiatives at both academic and industrial levels. Cybersecurity has become so vital in our daily lives that it needs to be introduced in elementary schools with basic knowledge to benefit the entire society. If society as a whole is not well-informed and trained, it can be vulnerable to cyberattacks. *Researchers have discussed the following factors that influence humans’ vulnerability to cyberattacks (Morgan et al., 2020):*

- *Cognitive factors:* low awareness, poor perception, limited understanding and knowledge.
- *Organisational/environmental factors:* weak security culture, work pressure, and stress.
- *Workload/stress factors:* time pressure, high workload, multitasking, cognitive overload, fatigue, and financial stress.
- *Decision-making biases:* availability heuristic, framing effect, sunk-cost fallacy, affect (emotion-driven) heuristic, truth-default bias.
- *Individual differences:* high trust, impulsivity, low self-control/awareness, risk-taking, self-deception, low expertise, strong need for affiliation.
- *Individual contextual factors:* cognitive overload, time pressure, financial need, fatigue, and other unsafe organisational cultures.

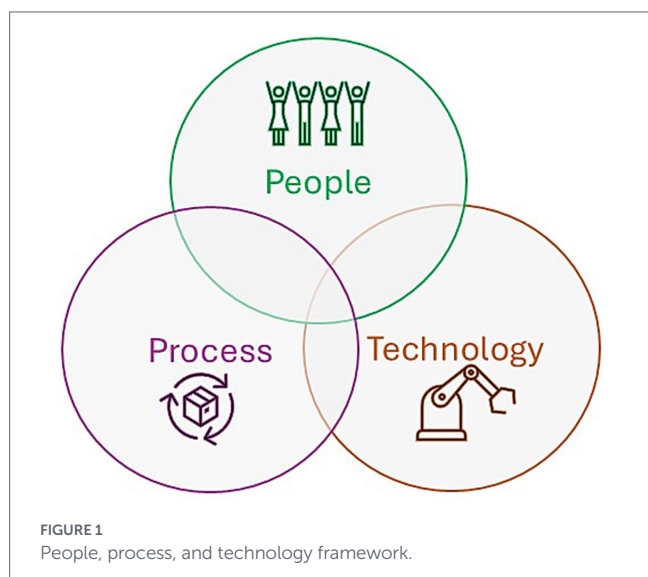
Other cognitive and psychological aspects of cybersecurity include cognitive biases (such as overconfidence and anchoring bias), risk perception (lack of recognising the severity of cyber threats), and lack of awareness and training (poor cyber hygiene) (Ayodele et al., 2025). Therefore, it becomes very important for the organisations to communicate about socio-technical cyber hygiene at workplaces rather than only technical hygiene (Morgan et al., 2020).

1.2 Instances of cyberattacks happened due to human error or negligence

Europe is facing an increase in cyberattacks, as its digital and economic strength makes it a prime target for cybercriminals. The UK reported 1.3 million computer misuse cases and a 33% rise in fraud in 2024, while Germany suffered \$298 billion in damages from cybercrime, primarily due to data theft and sabotage (Tamzid, 2025). France reported a 30% increase in ransomware attacks, with threats originating from Russia and China (Tamzid, 2025). With global cybercrime projected to cost \$10.5 trillion annually by 2025, robust cybersecurity practices, awareness, and collaboration are crucial for mitigating financial losses, operational disruptions, and reputational damage (Tamzid, 2025). Humans play a vital role in promoting

TABLE 1 Definitions of human-centric cybersecurity as provided in the literature.

Papers	Definition of human-centric cybersecurity
Mohammed (2025)	“Shifts the focus from purely technical solutions to an <i>integrated approach</i> that considers human behavior, motivations, and cognitive patterns.”
Khadka and Ullah (2025)	A <i>holistic framework</i> that integrates psychological, educational, organisational, and socio-technical dimensions to align human factors with technology and strategies, enhancing cybersecurity resilience.
Khadka and Ullah (2025)	An <i>approach</i> that goes beyond technical solutions by focusing on human behaviour, vulnerabilities, training, and organisational culture to enhance cybersecurity and reduce risks.
Gavaza and Katsande (2023)	“A <i>collection of the necessary knowledge and skills</i> required to create a capable workforce that can provide security safeguards, and develop, implement and enforce policies, standard operating procedures, tools, technologies and guidelines for best practices.”
Rao (2024)	An <i>emerging paradigm</i> that seeks to safeguard individual rights and freedom in cyberspace.
Grobler et al. (2021)	<i>Intangible concept</i> , involving all aspects of cyber security, with a particular focus on the human involvement, where humans represent both value and risk to an organisation. The focus is on the user, usage, and usability.
Rahman et al. (2021) and Rohan et al. (2021)	A <i>vague concept</i> based on the Computer Science (CS) community’s perspective of human factors, focusing on human involvement in processes and systems, their role, value, risks, and influence on cybersecurity goals. The focus is on user, system, and usability.
Rohan et al. (2021)	A <i>complicated concept</i> that encompasses consumer electronics (CE) and consumer technology (CT) is challenging to define due to the inherent relationships between humans and technology. The focus is on user, system, and usability.
Deibert (2018)	An <i>emerging approach</i> that prioritises human rights (such as access to information, freedom of thought, and freedom of association) over traditional security-centric models.



cybersecurity hygiene and bridging the gap between technology and users through proper training and awareness, as well as a strong organisational culture. History shows that cyberattacks have been caused by humans (insider threats), with malicious or non-malicious intent. According to MITRE, human-focused insider threat types include (DTEX, 2025):

- **Malicious insider:** These include insiders who seek to cause harm to the system.
- **Non-malicious insider:** These include negligent insiders (who know but do not care), mistaken insiders (who unintentionally create risk through genuine errors), and outsmarted insiders (who are manipulated by adversaries using novel tactics).
- **Coerced insider.** This is someone who initially has no malicious intent, but neither acts entirely non-maliciously. Instead, it is someone who is pressured, threatened, blackmailed, or otherwise

manipulated by a third party into carrying out harmful actions (Duncan et al., 2012). The very different types, and the third in particular, demonstrate that psychological factors are highly relevant to both understanding how cyber attacks are carried out and preventing them at the level of human interaction.

Organisations are increasingly at risk due to employees who lack proper training on security laws, device protection, and data handling. Common issues include sending confidential data to unsecured locations in the cloud, bypassing security policies to simplify tasks, and failing to update systems (DTEX, 2025). A global study in 2025 found that “insider threat risk” costs hit \$17.4 M, driven by post-incident expenses, with 7,868 incidents (23/org), mostly negligent (55%, caused by employee or contractor negligence/mistakes), and data breaches involving credentials (47%) and PII (47%) (DTEX, 2025). From this, we can deduce that people do not follow security policies due to the complexities of using such systems, which exposes organisations to cybersecurity risks. There are several notable instances of cyberattacks that have occurred globally due to human error or negligence. These include:

- **Uber Breaches (2014 and 2016):** Due to cloud credentials exposed on GitHub, Uber suffered a data breach containing sensitive information about the users (Paljug and Mikac, 2020).
- **WannaCry Ransomware Attack (2017):** Due to the negligence of not updating the Microsoft Windows operating system, around 300,000 + computers across 150 countries became victims of this ransomware attack, and the ransomware demanded around US\$300–600 (Mohurle and Patil, 2017).
- **Cash App Data Breach (2021):** A disgruntled ex-employee leaked Cash App’s customer data related to 8.2 M customers in the USA (CNN, 2022). Then again, in 2023, there was an unauthorised access to Cash App data. Customers of this app took the company to court, and it was ordered to pay a \$15 million cash settlement (Salinas, 2025).

- *Colonial Pipeline Ransomware Attack (2021)*: Due to negligence, such as unpatched and outdated systems, a leaked password led to the attack. After a hacker group obtained this password from the dark web, they directly accessed the network, as there was no two-factor authentication in place, which led to fuel delivery disruptions and panic buying across the United States (Beerman et al., 2023).
- *Tesla (2023)*: Due to negligence in revoking employees' access permission, two former employees of Tesla shared the confidential data with a German newspaper, affecting 75,735 people (Eva Rothenberg, 2023).
- *AI deepfake Attack (2024)*: In 2024, UK design and engineering company Arup, which is behind world-famous buildings such as the Sydney Opera House, was the target of an AI deepfake scam in which one of the employees sent \$25 million to criminals based on a video call with a senior management member (Magramo, 2024).
- *Louvre incident (2025)*: In October 2025, thieves managed to steal eight pieces of French crown jewels from the Louvre Museum. Investigators revealed that the museum's internal video surveillance system was protected by the password "Louvre." A confidential audit by France's National Cybersecurity Agency (ANSSI) already warned in 2014 that weak passwords and outdated systems created "serious shortcomings" in the museum's security (Bryony Gooch, 2025).

To address the aim of this study and provide a structured human-centric perspective on cybersecurity, this paper is guided by the following three Research Questions (RQ). These questions align with the adopted PRISMA-based methodology, the analysis of existing literature, and the evaluation of user perceptions of cybersecurity measures, with a particular focus on balancing security and ease of use.

- RQ1: What trends exist in human-centric cybersecurity research from the last decade, i.e., from 2015 to 2025?
- RQ2: How do users experience and perceive cybersecurity measures in their daily digital lives, particularly in terms of usability and security?
- RQ3: How can the integration of Industry 5.0 principles and the adoption of a triangle of People, Processes, and Technology support human-centric, resilient, and sustainable cybersecurity?

The remainder of this paper is organised as follows. Section 2 outlines the research methodology, specifically the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, which was selected for this review. Section 3 presents the results, including trends in human-centric research and the introduction of the human-centric cybersecurity framework as well as results from an online survey, providing an overview of how people experience and perceive cybersecurity in their daily digital lives, with a focus on the balance between security and ease of use. Section 4 presents a summary and observations, while Section 5 explores future directions, and Section 6 concludes the study.

2 Research methodology

This study followed Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology (Moher et al.,

2009) for a transparent and unbiased systematic review. Figure 2 illustrates the literature review process conducted following the PRISMA framework. The PRISMA approach includes several key components: defining eligibility criteria, identifying information sources, executing the search process, selecting relevant studies, and collecting and analysing data to present the results.

2.1 Eligibility criteria

Articles considered for this paper must meet the following inclusion and exclusion criteria see Table 2.

2.2 Information sources

To identify relevant literature on human-centric cybersecurity, the authors conducted searches across four databases: Google Scholar, Scopus, Web of Science, and IEEE Xplore, with most of the relevant studies found in Google Scholar.

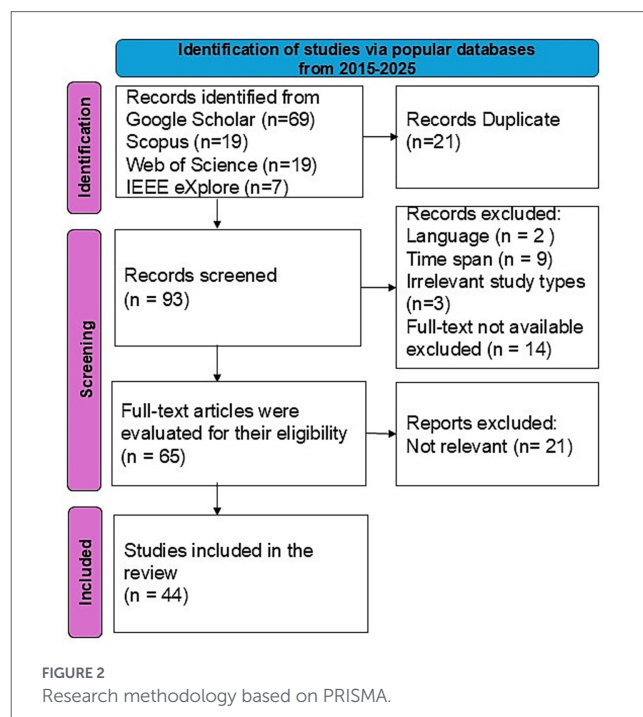
2.3 Search strategy

To determine the initial scope of human-centric cybersecurity, the authors conducted a web-based search using prominent academic databases as mentioned above.

The search query/string applied for the titles of the paper is: ("user-friendly security") OR ("user-friendly cybersecurity") OR ("human-centric cybersecurity") OR ("human-centric security").

2.4 Study selection

This review paper focuses on the domain of human-centric cybersecurity. All identified literature was consolidated to remove duplicate entries, resulting in a final selection of 44 papers based on predefined eligibility criteria (See Table 2) and relevance. These papers were then



thoroughly analysed with particular attention to the tools, technologies, methodologies, and application sectors discussed within them.

The focus is, thereby, not solely on the substantive content or explanatory depth of previous papers and studies. The act of mentioning and discussing is itself treated as an empirical and theoretical phenomenon. Specifically, the review treats descriptions and mentions in literature as objects of analysis in their own right, examined initially independent of their contextual and interpretive meanings. By foregrounding how concepts are repeated or positioned across papers, the review aims to hint at and, finally, reveal structural patterns, implicit assumptions and, ultimately, reveal silences in the field. This perspective allows us to, in future studies, fill gaps as to what “annoying cybersecurity” actually means and, ultimately, find out how to prevent it from being perceived as such. In essence, we presume human-centric

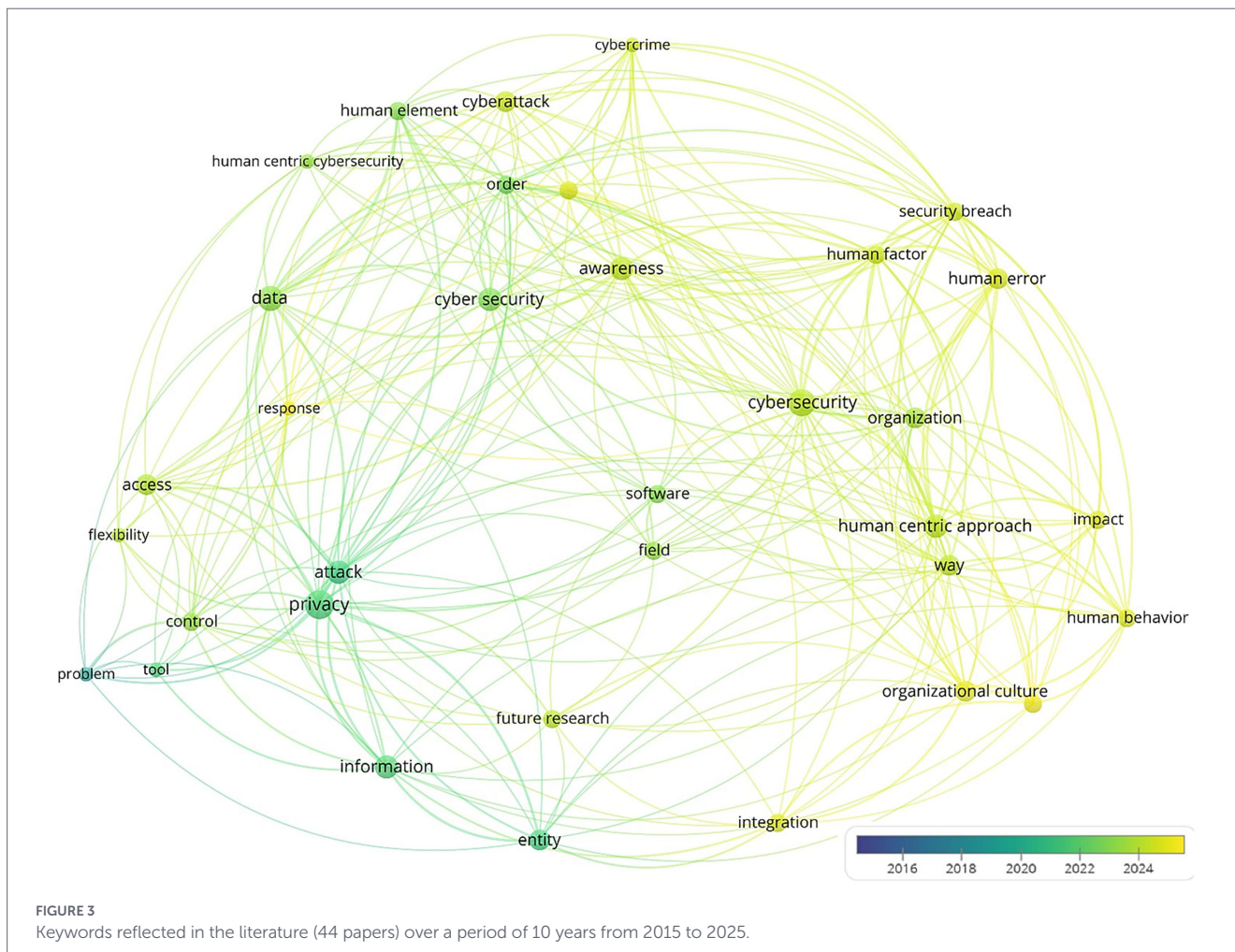
cybersecurity to be the exact opposite of annoying cybersecurity (Tables 3–7).

2.5 Data collection and analysis of results

The quality assessment of the identified literature for bias and rigor was a critical component of this systematic review. The web-based search strategy employed across the selected databases is illustrated in Figure 2, with the specific search strings detailed in Section 2.3. Most of the identified literature was sourced from the Google Scholar database, supplemented by other reputable databases like Scopus, IEEE Xplore, and Web of Science. Each study was evaluated by independent researchers, ensuring that only those meeting well-defined inclusion criteria were included in the analysis, thereby

TABLE 2 Inclusion and exclusion criteria for the current study.

Inclusion criteria	Exclusion criteria
<ul style="list-style-type: none"> • Studies published within a decade (i.e., 2015–2025). • Accessibility of the complete manuscript through Google Scholar and Scopus • Study type includes, e.g., peer-reviewed journal articles, conference papers, theses, and systematic reviews. • Studies published in English. • Studies focusing on human-centric and user-friendly cybersecurity. 	<ul style="list-style-type: none"> • Studies published outside the selected date range (i.e., 2015–2025). • Irrelevant study types, such as editorials, commentaries, and letters to the editor. • Unpublished manuscripts and non-peer-reviewed sources. • Language restrictions, such as studies not published in the English language. • Studies not focusing on human-centric and user-friendly cybersecurity.



reducing selection bias. After removing duplicates and irrelevant materials, a total of 44 papers published between 2015 and 2025 were selected for review.

To ensure the robustness of this systematic review, several validity threats were addressed, including selection bias, mitigated by clear eligibility criteria and the use of multiple reputable databases (Google Scholar, Scopus, IEEE Xplore, and Web of Science). Limitations, such

as restricting studies to English and a specific timeframe, were acknowledged as potential exclusions of relevant works. Information bias, stemming from limited search queries, was minimised through consensus meetings among researchers, with three independently analysing and resolving discrepancies in selected papers. Adhering to the PRISMA method, the review assessed 44 studies for quality and relevance, focusing on human-centric cybersecurity. The selected

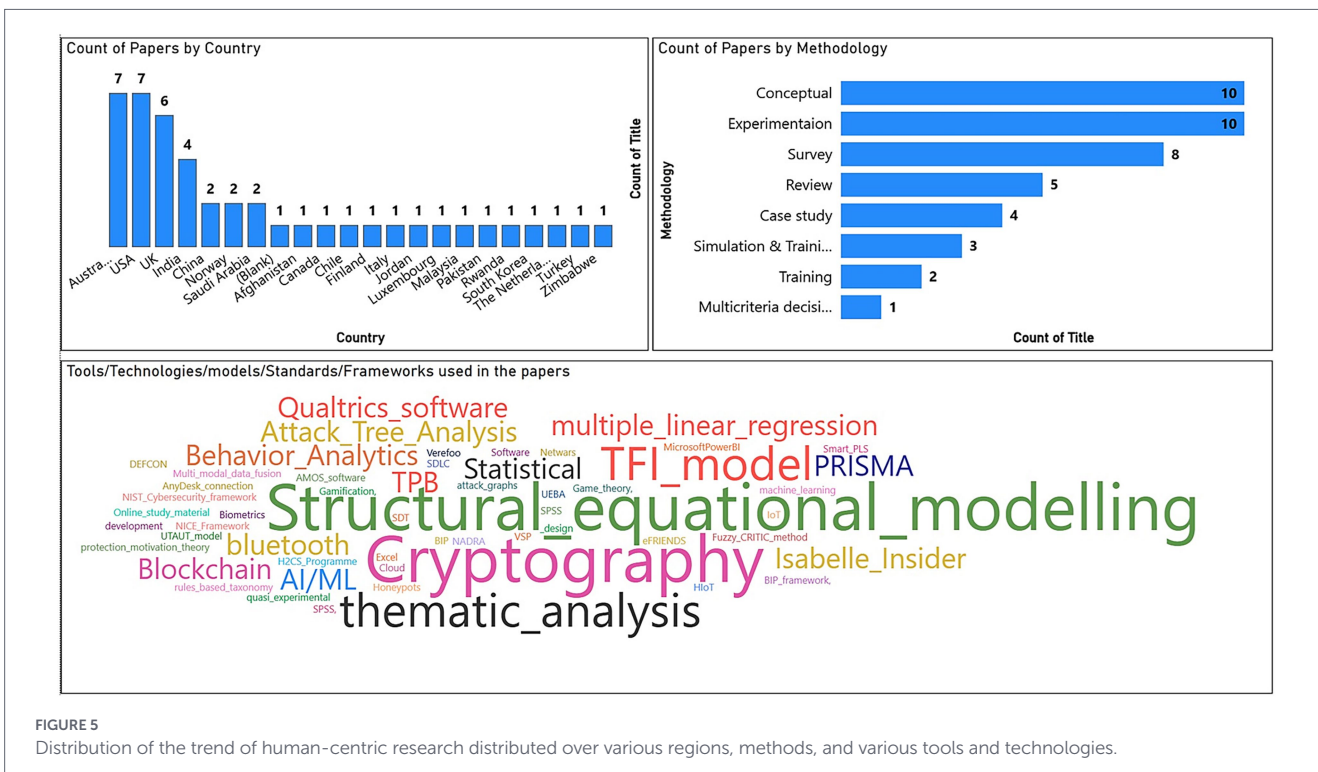
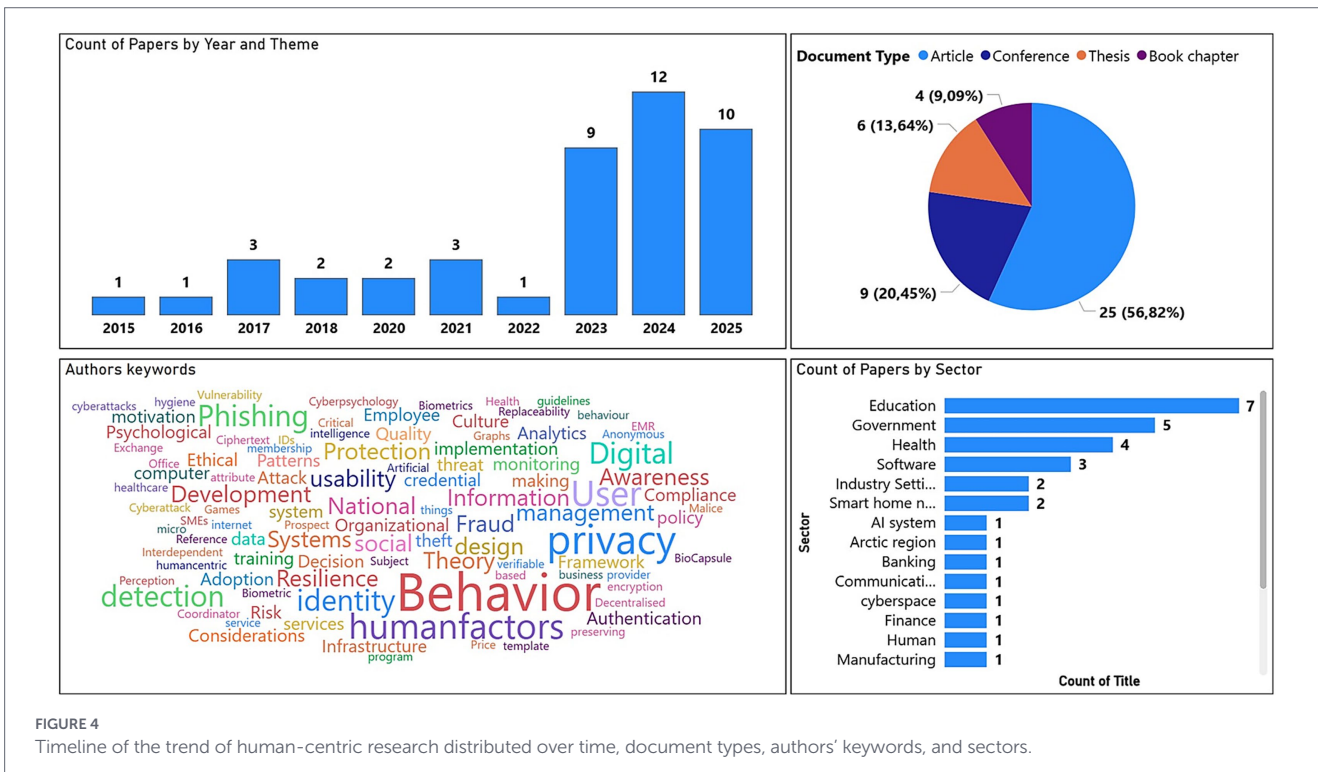


TABLE 3 Summary of observations of papers based on frameworks and policies.

Paper	Methodology	Sector	Tools/technologies/ models/standards/ frameworks	Outcome
Abdallah et al. (2025)	Experimental	Not defined	Game theory and attack graphs	This paper introduces a proactive security framework for analysing security decision-making in interdependent systems, utilising attack graphs to capture the impact of selfish and malicious defenders.
Mohammed (2025)	Conceptual	Organisational settings	UEBA (User and Entity Behavior Analytics)	This book chapter emphasises that integrating behavior analytics and machine learning with human-centric cybersecurity policies enhances proactive insider threat detection and brings a culture of trust and awareness within an organisation.
Tari and Mahmud (2025)	Experimental	Not defined	Multi-modal data fusion and a rules-based taxonomy and machine learning	This paper presents an analytical system that integrates multimodal data (such as user activity logs and behavioural indicators) with a rules-based taxonomy, improving cybersecurity measures by 11.25% while increasing user acceptance by 15.22%, offering a robust and human-centric security framework.
Zhou and Wang (2025)	Experimental	Maritime	AI/ML models	This paper introduces a novel and adaptive cybersecurity framework explicitly designed for the maritime domain, addressing human factors.
Ryan (2025)	Experimental	Government	Cryptography	This paper discusses the security protocols, especially in voting systems that must be designed with human usability in mind, balancing simplicity and trust by applying the KISS (Keep It Simple, Stupid) principle.
Troublefield (2025)	Surveys and interviews	SMEs	Statistical and thematic analysis	This paper reveals strong correlations between psychological and organisational factors influencing cybersecurity in SMEs, showing that self-efficacy, positive attitudes, and social norms significantly enhance compliance. In contrast, policy complexity, communication gaps, and resource constraints reduce cybersecurity effectiveness.
Kurdi et al. (2024)	Survey	Software	Software development life-cycle (SDLC)	This paper highlights the necessity of enhancing security awareness among all members of software development teams from the early stages of the SDLC to strengthen both software quality and security.
Al Ansari et al. (2024)	Review	AI system and PRISMA method	Not defined	This paper promotes for a human-centred design approach to AI systems, enabling easy use while maintaining data privacy and security.
Ozkan Ozen et al. (2024)	Multicriteria decision making (MCDM)	Manufacturing	Fuzzy CRITIC method	This paper identifies three major human-centric cybersecurity risks within the manufacturing industry: employee resistance to cybersecurity practices and data privacy measures, insufficient employee training and education, and inadequate integration between humans and machines.
Rishiwal et al. (2024)	Review	Vehicle communication and PRISMA method	AI/ML models	This paper proposes a blockchain-based, human-centric security framework that ensures authorised access to Vehicle-to-Everything (V2X) communication networks, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Network (V2N) communication.
van der Kleij et al. (2024)	Conceptual	Software	Not Defined	This paper highlights the need for human-centric security engineering that balances usability and cybersecurity, integrates organisational culture, and investigates the interplay between organisational elements and cybersecurity culture in practice.

(Continued)

TABLE 3 (Continued)

Paper	Methodology	Sector	Tools/technologies/ models/standards/ frameworks	Outcome
Dikito and Kaiser (2023)	Survey	Banking	SPSS 23, Smart PLS Version 3.2.8, SEM	This paper indicates that human factors (awareness, cybersecurity policy, and top management) have a direct and negative impact on identity theft.
Tabari (2021)	Experimental	Communication networks	IoT devices and Honeybots	This thesis has proposed an Internet of Things honeypot framework (MPMFPot) to observe attackers' behavior within a controlled environment.
Morgan et al. (2020)	Conceptual	Industry Settings	Airbus Accelerator in Human-Centric Cyber Security (H2CS) Programme	This paper discusses how human-centric cybersecurity research within organisations enhances understanding of human vulnerabilities and enables socio-technical practices that strengthen overall cyber hygiene.
Klein and Hossain (2020)	Conceptual	Arctic region	Not defined	This paper discusses how digitalisation and climate change jointly reshape the Arctic, highlighting the need for cybersecurity to be human-centric. This includes safeguarding people's privacy, access, and critical services while leveraging digital tools (e.g., social media, online platforms) to expand participation, resilience, and cultural preservation.
Hussain (2017)	Review	Government	NADRA (National Database and Registration Authority)	This paper presents a framework for detecting web vulnerabilities, monitoring traffic, utilising modern web tools, executing a six-step scan with four testing stages, and displaying outcomes.

studies originated from high-quality, peer-reviewed journals, which not only enhanced the credibility of the findings but also underscored the rigor of the evaluation process.

Given that human-centric cybersecurity is an emerging field with limited available research, the scope of this paper is confined to exploring this specific area rather than offering a comprehensive or critical literature review, utilising primarily four databases. Future research, however, could very well extend this scope and explore human-centric cybersecurity in a continuously and ever-changing landscape.

3 Results

3.1 Trends in human-centric research

This section presents results from the literature, illustrating the trend in human-centric research over a decade from 2015 to 2025. We used VOSviewer in Figure 3 to analyse the keywords used by the authors of the 44 reviewed papers.

Figure 3 is a keyword co-occurrence network visualisation showing the evolution and interconnections of major research themes in the domain of human-centric cybersecurity over time. Each node represents a keyword, and the node's size indicates its frequency or importance within the dataset, while the lines (edges) between nodes reflect how often those terms co-occur. The colour gradient, ranging from blue (2015) to yellow (2025), illustrates the temporal progression of topics. Early research (blue-green nodes such as privacy, attack, data, and access control) focused on technical and data-centric issues. In contrast, more recent studies (yellow

nodes such as human error, human behaviour, human factor, awareness, and organisational culture) emphasise the human and organisational aspects of cybersecurity. This shift highlights a growing recognition of the critical role of human factors and culture in maintaining cybersecurity resilience.

Figure 4 (Top left) Illustrates a significant upward trend in human-centric research publications over time. The years from 2015 to 2022 exhibit limited research activity, but a steady increase begins in 2023, indicating a growing global focus on human-centric cybersecurity.

Figure 4 (top right) shows that it is distributed across academic journals (57%), conferences (20%), theses (14%), and book chapters (9%). Figure 4 (bottom-left) presents an analysis of keywords used in the reviewed literature, revealing a focus on terms such as behaviour, privacy, human factors, digital identity, usability, psychological, and others. We have excluded "human-centric" and "cybersecurity" keywords, as they appear with the highest frequency due to their prominence in our search criteria. Additionally, Figure 4 (bottom right) shows that the education and government sectors lead with the highest focus at 16 and 11%, respectively, followed by the health sector at 9% and the software sector at 7%. Overall, the analysis reveals that cybersecurity research is most concentrated in education, governance, and healthcare, reflecting a growing focus on human-centric and policy-driven security approaches in these key sectors.

The final 44 papers in the literature provide an overview of human-centric cybersecurity research from 21 countries. Figure 5 (top left) shows that most contributions originate from Australia, the USA, and the UK, collectively accounting for approximately half of the research. Other notable contributors include India, China, and Norway. Next, Figure 5 (top right) represents that these contributions are well-balanced, with conceptual, experimental, and survey

TABLE 4 Summary of observations of papers based on authentication and identity.

Paper	Methodology	Sector	Tools/technologies/ models/standards/ frameworks	Outcome
Hilowle et al. (2024)	Survey	Government	SEM, multiple linear regression analysis, TFI model, theory of planned behavior (TPB), and Qualtrics software	This paper identifies that security, privacy, usability, flexibility, and cultural-social factors significantly influence Australians' intention to use national digital identity systems (NDIDs), while trust and cybersecurity awareness do not.
Wang (2024)	Experimental	Health	Blockchain, Cloud, and Cryptography	This paper proposes a blockchain-based system that securely protects patient data, facilitates the easy and private sharing of medical records, and operates efficiently.
Muhudin Hilowle (2023)	Survey	Government	SEM, multiple linear regression analysis, TFI model, theory of planned behavior (TPB), Qualtrics software, and Thematic analysis	This thesis shows that users adopt national digital identity systems (NDIDs) when they are secure, private, flexible, and easy to use, but low trust, poor cybersecurity awareness, and social or cultural concerns reduce adoption.
Marino (2023)	Experimental	Smart home network	Verefoo (Verified Refinement and Optimized Orchestration) framework	This thesis extends the Verefoo framework to enable the automatic allocation and configuration of Parental Control Systems, addressing a critical challenge within the context of home networks.
Hilowle et al. (2023)	Review	Government	Technology formal informal (TFI) model, unified theory of acceptance and use of technology (UTAUT) model	This paper proposes a multi-level conceptual framework that offers opportunities to contextualise human-centric cybersecurity factors influencing user adoption of NDID.
Ra et al. (2021)		Human	Human Internet of Things (HIIoT) and blockchain	This paper proposes a human-centric identity management system (IDM) system based on blockchain and zero-knowledge proof (ZKP) for privacy preservation in the HIIoT environment.
Lakshmisree (2016)	Experimental	Not defined	Biometrics	This paper presents a user-friendly authentication mechanism to secure biometric information.

approaches each accounting for approximately 64% of the total, indicating a mature blend of theoretical and applied research.

Furthermore, [Figure 5](#) (bottom) shows a word cloud of tools/technologies/standards/frameworks used across human-centric cybersecurity research. Most of the research applies Structural Equation Modelling (SEM) ([Dikito and Kaiser, 2023](#); [Hilowle et al., 2024](#); [Jamil et al., 2025](#); [Muhudin Hilowle, 2023](#)), cryptography ([Kammüller, 2018](#); [Kammüller et al., 2017](#); [Ryan, 2025](#); [Wang, 2024](#)), thematic analysis ([Muhudin Hilowle, 2023](#); [Tambe-Jagtap, 2023](#); [Troublefield, 2025](#)), Technical Formal Informal (TFI) model ([Hilowle et al., 2023, 2024](#); [Muhudin Hilowle, 2023](#)), Blockchain ([Ra et al., 2021](#); [Wang, 2024](#)), behaviour analytics ([Mohammed, 2025](#); [Narayanan and Srinivasan, 2025](#)) and others.

3.2 Review results by research themes

[Figure 6](#) presents the timeline of publications from 2015 to 2025, providing an overview of research in human-centric cybersecurity across five key themes. The themes, along with the number of literatures within each theme, include frameworks and policies (16), education and training (8), human factors (8), authentication and identity (7), and usability and privacy (5). In the year 2024, frameworks and policies dominated ([Al Ansari et al., 2024](#); [Kurdi et al., 2024](#); [Ozkan Ozen et al., 2024](#); [Rishiwal et al., 2024](#); [Troublefield, 2025](#); [van der Kleij et al., 2024](#)), accounting for half of all papers, followed by notable contributions on human factors ([Gjertsås, 2024](#); [Hakimi et al., 2024](#); [Jamil et al., 2025](#); [Rao, 2024](#)) and authentication

and identity ([Hilowle et al., 2024](#); [Wang, 2024](#)). A similar pattern emerged in 2025, where frameworks and policies once again took precedence ([Abdallah et al., 2025](#); [Mohammed, 2025](#); [Ryan, 2025](#); [Tari and Mahmud, 2025](#); [Zhou and Wang, 2025](#)), but this time with an added emphasis on education and training ([Bush and Mashatan, 2025](#); [Jethava et al., 2025](#); [Kelechukwu et al., 2025](#)). This shift indicates a maturing research landscape, moving from isolated, technical studies toward more comprehensive, policy-oriented, and human-centred investigations. The refined results for each theme are presented in sections 3.2.1–3.2.5.

3.2.1 Frameworks and policies

This theme, at around 36%, is the most dominant and shows that most human-centric cybersecurity research has led to the introduction of frameworks and policies. The focus of these studies is on developing structured, strategic approaches that integrate human factors into cybersecurity practices across multiple sectors, including government and software. The frameworks commonly emphasise behaviour, psychological resilience, awareness, risks, digitalisation, and quality as key components, aiming to improve risk management, digital ecosystem, and organisational security culture. Methodologically, conceptual and experimental approaches are applied, reflecting a balance between theory development and practical validation. The reviewed literature within this theme uses analytical tools and standards, such as PRISMA ([Al Ansari et al., 2024](#); [Rishiwal et al., 2024](#)), AI/ML-based models

TABLE 5 Summary of observations of papers based on human factors.

Paper	Methodology	Sector	Tools/technologies/ models/standards/ frameworks	Outcome
Narayanan and Srinivasan (2025)	Experimental	Finance	Behaviour Analytics	This paper presents that a Hybrid human-centric cybersecurity (AI + human insight) approach using behavioural analytics significantly improves detection and prevention of phishing, credential theft, and social engineering while reducing errors and enhancing user experience in financial services.
Jamil et al. (2025)	Survey	Market Research	Protection Motivation Theory (PMT)-based model, SEM, SPSS version 26 and the AMOS software	This paper presents a research model based on PMT, demonstrating that all protection motivation constructs except threat susceptibility effectively predict users' protective behaviours. Additionally, it finds that higher cybersecurity costs negatively influence users' engagement in safe cyber practices.
Ayodele et al. (2025)	Conceptual	Not defined	Not defined	This paper discusses various human vulnerabilities and proposes a multi-faceted approach to enhance human-centric cybersecurity using AI tools and training programs.
Hakimi et al. (2024)	Conceptual	Not defined	Not defined	This paper emphasises that a human-centric approach, integrating technology with an understanding of human behaviour and cognition, is essential for building effective and resilient cybersecurity systems.
Rao (2024)	Case study	Cyberspace	Not defined	This thesis examines the significance of human rights in the cyber domain, taking into account various geopolitical contexts. It discusses the need for creating a balanced cybersecurity strategy to protect both national security as well as individual rights.
Gjertsås (2024)	Case study	Industry Settings	Self-Determination Theory (SDT), Visma Security Program (VSP), and Microsoft PowerBI	This thesis found that applying Self-Determination Theory (autonomy, competence, and relatedness) in organisational security programs boosts employee motivation, improves security compliance, and reduces human error.
Tambe-Jagtap (2023)	Surveys and interviews	Education	Statistical and thematic analysis	This paper presents a human-centred cybersecurity program that integrates AI tools to significantly reduce errors, response times, and breach costs while enhancing security.
Gopireddy (2022)	Conceptual	Not defined	Not defined	This paper discusses human behaviours and ethical considerations to enhance cybersecurity.

(Rishiwal et al., 2024; Zhou and Wang, 2025), Game Theory (Abdallah et al., 2025) and SDLC (Hadi, 2023; Kurdi et al., 2024), highlights a systematic, data-driven orientation in this category. Overall, this theme emphasises a shift toward human-centric cybersecurity principles through standardised, policy-oriented cybersecurity frameworks.

3.2.2 Education and training

Within this theme, 8 of 44 papers (18%) were identified that focus on developing and enhancing cybersecurity awareness and skills through structured programs (Coffey et al., 2018; Kassicieh et al., 2015), frameworks (Gavaza and Katsande, 2023), and training tools like NetWars (Depassier and Torres, 2018). Of these eight papers, six focus on the education sector, one addresses health (Kioskli et al., 2023) and another explores smart home networks (Bush and Mashatan, 2025). Collectively, these papers emphasise the importance of human-centric education for organisational employees, smart home users, and both technical and non-technical users. Such education improves cyber hygiene and helps

mitigate breaches caused by human error and lack of awareness. Moreover, the methodology distribution reveals a firm reliance on training and conceptual approaches, indicating that much of this research focuses on designing and testing educational models or conceptual frameworks rather than purely technical solutions. Together, these works highlight the critical role of education, training, and continuous skill development in fostering a resilient cybersecurity culture.

3.2.3 Human factors

Within this theme, 8 out of 44 papers (18%) were identified that highlight the growing emphasis on a human-centric approach to cybersecurity, integrating technology with an understanding of human behaviour, cognition, and motivation. The studies demonstrate that psychological frameworks such as Protection Motivation Theory (PMT) (Boer and Seydel, 1996) and Self-Determination Theory (SDT) (Deci and Ryan, 1980) effectively predict and enhance users' protective behaviours and compliance, while also showing that higher cybersecurity costs can discourage safe practices. Some literature proposes

TABLE 6 Summary of observations of papers based on education and training.

Paper	Methodology	Sector	Tools/technologies/ models/standards/ frameworks	Outcome
Bush and Mashatan (2025)	Conceptual	Smart home network	Not defined	This book chapter provides some recommendations based on a collaborative approach following human-centric principles for smart home users, vendors, and policy-makers.
Kelechukwu et al. (2025)	Simulation and training	Education	Gamification	This paper finds that human-centric cybersecurity training significantly outperforms traditional methods by driving sustained behavior change, markedly improving engagement, self-efficacy, secure behavior adoption, knowledge retention, and phishing resilience.
Jethava et al. (2025)	Simulation and training	Education	AI/ML	This book chapter proposes a toolbox that can help both technical and non-technical users to identify vulnerabilities while using Internet.
Gavaza and Katsande (2023)	Training	Education	NIST Cybersecurity framework and NICE Framework	This book chapter redesigns a cybersecurity framework by combining the NIST and NICE frameworks, further strengthened by supportive environments with national laws, institutional policies, and active industry associations that foster best practices and workforce development.
Kioskli et al. (2023)	Conceptual	Health	Not defined	This paper emphasises that improving cyber hygiene in healthcare requires human-centric education and practices addressing user behaviour, as most cyberattacks stem from human error and insufficient awareness of cybersecurity best practices.
Coffey et al. (2018)	Training	Education	Online study material	This paper presents a training program that has been implemented for the regional university employees. The training program contents include FERPA (Family Educational Rights and Privacy Act) basics, data Security and privacy, knowledge worker skills assessment, and understanding regarding confidentiality.
Depassier and Torres (2018)	Simulation and Training	Education	Netwars tool, DEFCON CTF 22 dataset, and AnyDesk connection software	This paper presents NetWars, a human-centric training tool that yielded 95% success rate in helping analysts prioritise multi-stage cyberattacks using DEF CON CTF data, with positive usability results.
Kassicieh et al. (2015)	Conceptual	Education	Not defined	This paper recommends a variety of cybersecurity awareness programs for training the current employees within an organisation.

AI-assisted, ethically grounded strategies to address human and social engineering vulnerabilities (Ayodele et al., 2025; Narayanan and Srinivasan, 2025), reduce security incidents, and balance national security with individual rights (Rao, 2024). Together, these studies reinforce the need for effective, resilient cybersecurity systems to prioritise human factors alongside technological innovation.

3.2.4 Authentication and identity

Within this theme, 7 out of 44 papers (16%) were identified that have explored diverse approaches to enhancing security, privacy, and user adoption in digital identity and authentication systems. Out of these, three papers (43%) focus on applications in the government sector (Hilowle et al., 2023, 2024; Muhudin Hilowle, 2023). The analytical tools and techniques employed across these studies include the technical formal-informal (TFI) model, structural equation modelling (SEM), multiple linear regression, and Qualtrics software (Hilowle et al., 2023, 2024; Muhudin Hilowle, 2023) as well as blockchain technologies (Ra et al., 2021; Wang, 2024). Methodologically,

three papers adopt experimental designs (Lakshmisree, 2016; Marino, 2023; Wang, 2024) while other papers are based on survey and review approaches. Collectively, studies in this theme advance human-centric, technology-driven models for secure, private, and user-friendly authentication and identity management solutions.

3.2.5 Usability and privacy

Within this theme, 5 of 44 papers (11%) were identified that focus on applying human-centric approaches to enhance cybersecurity design, usability, and trust across different sectors. Two case studies in the healthcare sector employed formal methods such as the Isabelle Insider Framework, Attack Tree Analysis, (Behaviour, Interaction, Priority) BIP framework, and Secure Simple Pairing (SSP) for Bluetooth to strengthen IoT security, privacy, and ethical compliance, ensuring end-to-end protection and insider risk detection (Kammüller, 2018; Kammüller et al., 2017). A review paper emphasised the need to shift from functional and usage-centric models toward a user-centric framework

TABLE 7 Summary of observations of papers based on usability and privacy.

Paper	Methodology	Sector	Tools/technologies/ models/standards/ frameworks	Outcome
Hadi (2023)	Surveys and interviews	Software	Secure Software Development Life Cycle (SSDLC)	This thesis suggests the need for integrating usability and cognitive cost considerations while developing cybersecurity solutions.
Grobler et al. (2021)	Review	Not defined	Not defined	This paper highlights that effective cybersecurity requires shifting from functional and usage-centric approaches to a user-centric model by integrating user, usage, and usability (the 3 U's) into security design, implementation, and deployment.
Kammüller (2018)	Case study	Health	Isabelle Insider framework, Attack Tree Analysis, BIP framework, cryptography, SSP for Bluetooth	This paper presents a formal methods approach using Isabelle to enhance security and privacy in human-centric IoT healthcare systems.
Kammüller et al. (2017)	Case study	Health	eFRIENDS ethical framework, Isabelle Insider framework, Attack Tree Analysis, BIP framework, cryptography, SSP for Bluetooth	This paper presents a formal method and ethical design that can enhance the security, privacy, and trustworthiness of IoT healthcare systems by detecting insider risks and implementing end-to-end encryption.
Alemerien (2017)	Experimentation	Social Network	Not defined	This paper finds that social network interfaces designed using the proposed user-friendly security patterns were more positively received and accepted by users compared to existing Facebook interfaces.

that integrates user, usage, and usability the “3 U’s” into cybersecurity design and deployment (Grobler et al., 2021). Other studies focus on incorporating user-friendly security interfaces into social media networks (Alemerien, 2017) and on including usability and cognitive cost considerations within secure software design processes (Hadi, 2023). Together, these studies highlight a growing focus on embedding human-centric designs and usability into cybersecurity systems to enhance both effectiveness and user trust.

3.3 Framework for human-centric cybersecurity

This section presents a framework for human-centric cybersecurity to enable Industry 5.0, in which humans have direct interaction with systems and solutions are more customer-oriented. The framework gathers insights from a straightforward survey conducted in Europe to understand how individuals experience and perceive cybersecurity in their everyday digital lives, focusing on the balance between security and ease of use.

3.3.1 Survey

We have conducted a simple and small user study, which is entirely exploratory in nature. We acknowledge that the comparably small sample size of 30 participants limits its statistical and prognostic power. Data has been collected through a well-structured anonymous questionnaire that aims to explore users' confidence in following security practices, which measures they find most annoying, and whether these factors affect productivity. The survey also gathers suggestions for making cybersecurity more user-friendly, helping to design security systems that protect effectively while remaining convenient and less disruptive. The findings primarily serve the illustrative purpose of identifying usability concerns rather than providing novel and

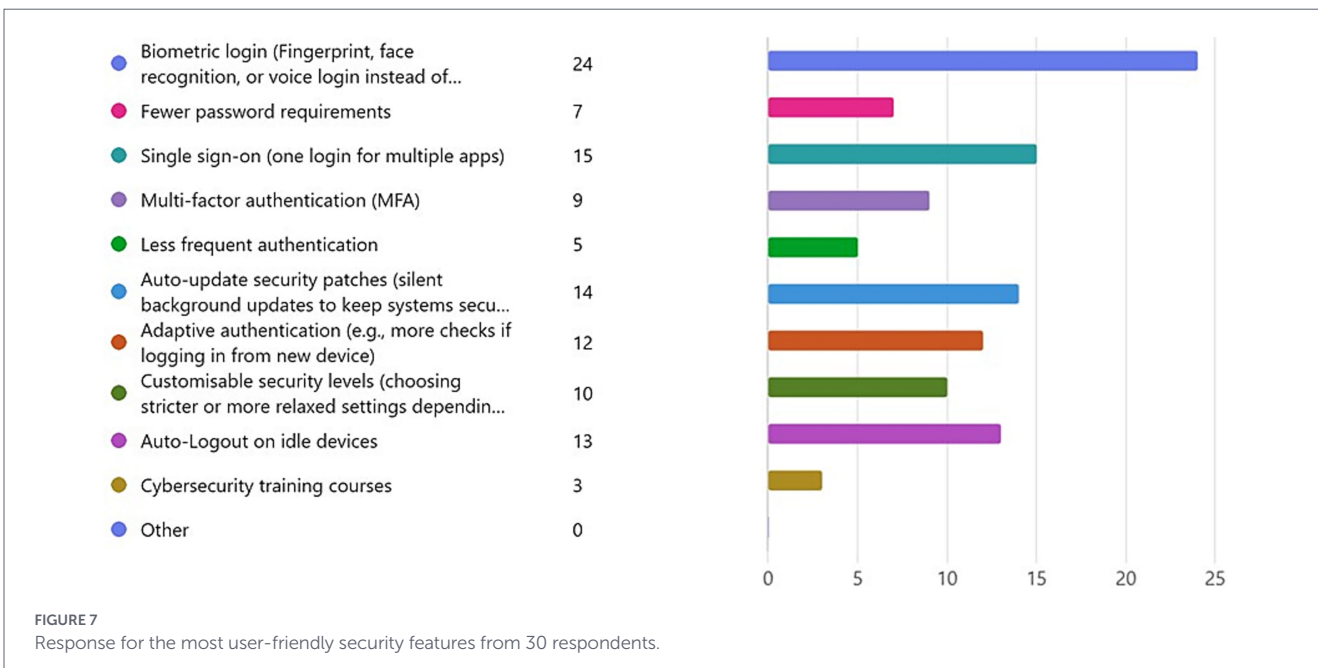
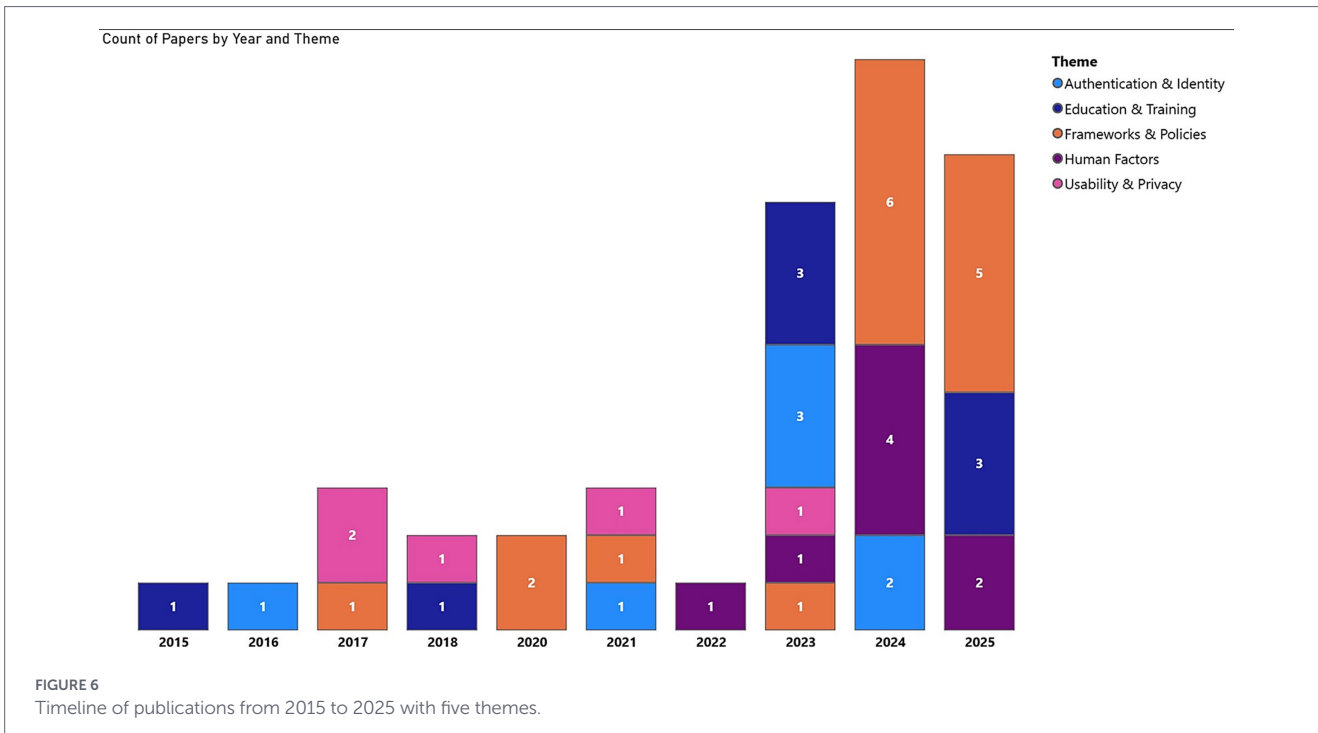
overall generalisable insights. It intends to contextualise the framework with lived user experiences.

The survey results are based on 30 respondents from Europe. The majority of the survey respondents are aged 31–50, with a small number under 30 or over 50. The survey respondents were split between women (47%) and men (53%). Most survey respondents work in the private sector (47%), followed by academia (30%), with a smaller representation from the public sector (10%) and other fields (13%). Most respondents (80%) considered cybersecurity extremely important, while others found it somewhat important. Responses were mixed: 30% of participants found cybersecurity measures annoying daily, and almost equal shares (27%) reported annoyance monthly or seasonally, while fewer reported annoyance weekly (7%), yearly (3%), or never (7%).

Respondents identified frequent password resets (33.3%) and frequent authentication (26.7%) as the most annoying cybersecurity measures, while security awareness training and system updates were rated as less annoying overall. Responses were evenly divided: 40% of participants believed cybersecurity measures reduce productivity, 43% said they do not, and 17% were unsure. Most respondents (46%) agreed and strongly agreed that secure systems are designed with user convenience in mind, while 27% disagreed and 27% remained neutral.

Most respondents (80%) found biometric login to be the most user-friendly security feature, followed by single sign-on (50%) and automatic security patch updates (46%), as shown in Figure 7.

Additionally, respondents suggested making cybersecurity more user-friendly by implementing simplified, built-in password managers, unified authentication systems such as biometrics, passwordless logins, or single sign-on (SSO). Many emphasised the need for fewer or more thoughtful MFA prompts (e.g., a number to confirm in the system rather than the ones we must type a given 6-digit number), less frequent password resets, and a universal digital ID or identity wallet.



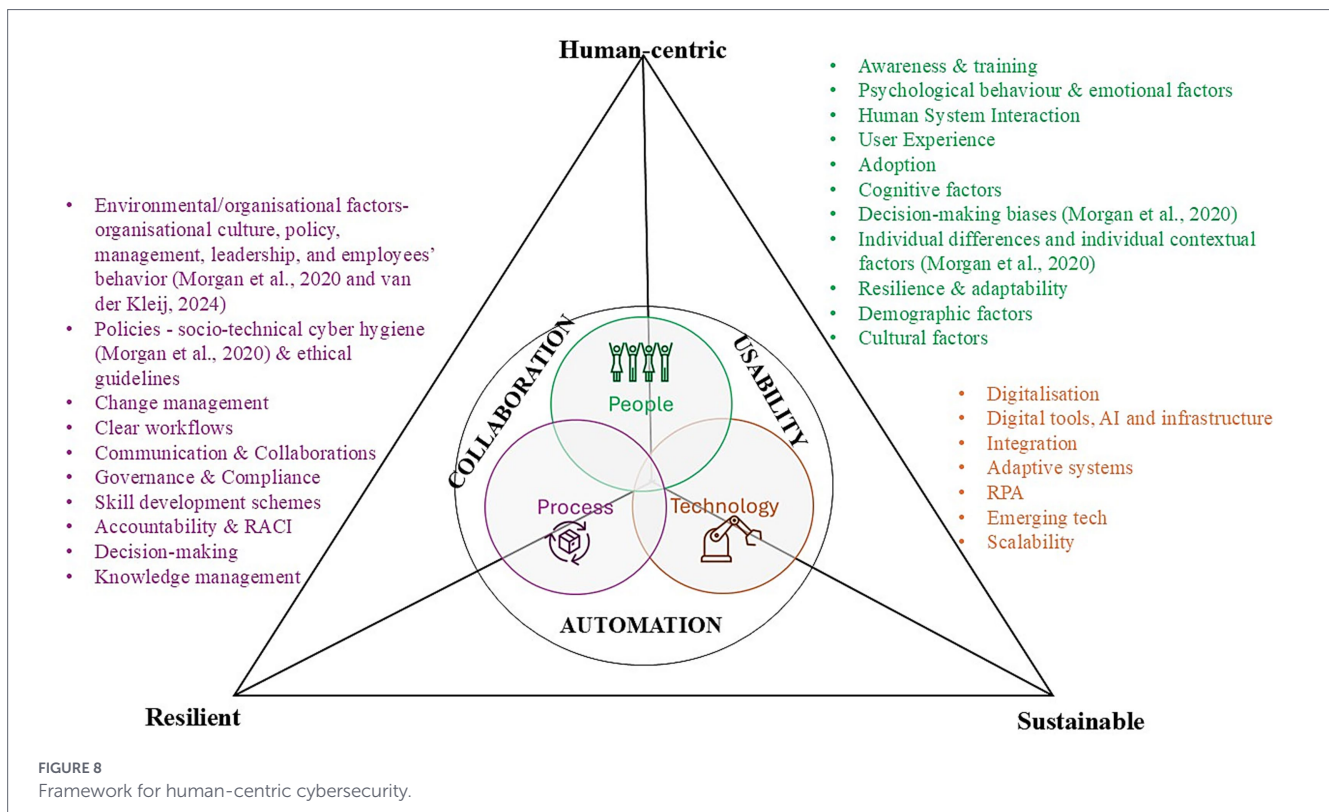
Others proposed more precise explanations and better-designed training, as well as automated background protection and AI-driven adaptive systems that maintain security without interrupting work. Overall, participants called for a balance between security and convenience, aiming for systems that are intuitive, seamless, and minimally intrusive.

The results from the survey provide valuable insights into the effectiveness of the proposed framework and highlight how participants perceive various aspects of cybersecurity in their daily lives. This feedback plays a crucial role in assessing the framework's strengths

and areas for improvement, ultimately guiding future enhancements and ensuring it meets user needs more effectively. Henceforth, these suggestions are categorised for mapping them to the proposed framework as discussed in Section 3.3.2.

3.3.2 Proposed framework

The proposed framework (See Figure 8) uses the People, Process, and Technology (PPT) model to demonstrate how these elements can be incorporated into a human-centric cybersecurity approach. When



we consider the interaction between these elements, we see three main aspects:

- 1 Usability represents the interface between People and Technology, ensuring systems are user-friendly, simple, and accessible.
- 2 Automation defines the connection between Technology and Process, enabling efficiency and consistency through intelligent systems.
- 3 Collaboration captures the link between People and Process, fostering teamwork, communication, and shared responsibility in maintaining security.

Together, these interactions form a balanced and adaptive framework that prioritizes human factors while leveraging technological and procedural strengths to achieve resilient cybersecurity in Industry 5.0. All factors influencing the PPT model in the proposed framework have been considered, based on the literature and the authors' experiences. It is also important to note that this framework is not intended to be applied statically or rigidly. For instance, elements of automation can emerge within the People-Technology interface when individuals interact with technology so naturally and routinely that the behaviour itself becomes automated. Similarly, collaborative dynamics can influence the Process-Technology interface, where processes continuously inform technological adjustments and, in turn, technologies shape or refine procedural workflows. This interplay becomes even more pronounced with the adoption of AI-driven methodologies, which further reinforce and enhance the collaborative dimension of the framework.

Additionally, we have conducted a PPT-based analysis, as shown in Table 8, that illustrates how the three elements of the

PPT Model of our framework are reflected in the reviewed literature.

This analysis shows a balanced distribution of the reviewed literature across all three dimensions. Additionally, in 2023 and 2024, research is largely concentrated on the People and Process elements, with a notable increase in People-focused studies in 2024. By 2025, a noticeable shift toward Technology-focused research is observed, indicating growing emphasis on technical solutions alongside human-centric considerations. This trend corresponds with increased concern over human-related cybersecurity risks and the expanding use of emerging digital technologies.

The theoretical basis for our framework is a core triad of human-centrism, resilience and sustainability, which was not mentioned by other researchers. It thereby draws on:

- The human-centric security elements that we have explored in the literature review, as well as
- Resilience theory emphasising the capacity to withstand and, especially, recover from cyber threats and
- Sustainability theory focusing on long-term viability and adaptability in an ever-changing threat landscape and technological environment.

In doing so, our framework is the first to explicitly integrate human-centrism, resilience and sustainability as equal and interdependent pillars to achieve true human-centric cybersecurity. This does not only entail an inherent shift from reactivity to proactivity through its long-term adaptive capacity to a technology-agnostic view of cybersecurity but also offers a very practical applicability. Compared to similar frameworks, it does not frame the human as a single point of failure, but a critical contributor to cyber resilience. With all three, people, processes and technology at its core, it is comprehensive and holistic.

TABLE 8 PPT-based analysis of the literature.

PPT model element	Description	Papers	Number of papers
People/human	Literature in this group examines the influence of human behavior, cognition, motivation, usability, skills, and decision-making on cybersecurity.	Abdallah et al. (2025); Al Ansari et al. (2024); Ayodele et al. (2025); Dikito and Kaiser (2023); Gjertsås (2024); Gopireddy (2022); Grobler et al. (2021); Hakimi et al. (2024); Hilowle et al. (2024); Jamil et al. (2025); Kelechukwu et al. (2025); Muhudin Hilowle (2023); Rao (2024); Tamba-Jagtap (2023); Depassier and Torres (2018)	15
Process	Literature in this group consists of organisational, managerial, and procedural mechanisms that guide cybersecurity implementation and governance.	Coffey et al. (2018); Gavaza and Katsande (2023); Hadi (2023); Hilowle et al. (2023); Hussain (2017); Kassicieh et al. (2015); Kioskli et al. (2023); Klein and Hossain (2020); Kurdi et al. (2024); Morgan et al. (2020); Ozkan Ozen et al. (2024); Tari and Mahmud (2025); Troublefield (2025); van der Kleij et al. (2024)	14
Technology	Literature in this group consists of technical tools, systems, architectures, and mechanisms used to implement security controls.	Alemieren (2017); Bush and Mashatan (2025); Jethava et al. (2025); Kammüller (2018); Kammüller et al. (2017); Lakshmisree (2016); Marino (2023); Mohammed (2025); Narayanan and Srinivasan (2025); Ra et al. (2021); Rishiwal et al. (2024); Ryan (2025); Tabari (2021); Wang (2024); Zhou and Wang (2025)	15

The suggestions from the 30 respondents helped in evaluating the framework's three main aspects as:

- **Automation:** Several responses focused on the idea of automating cybersecurity to make it easier and more efficient. People suggested systems that automatically detect threats, reduce the need for repeated logins, and handle security in the background without requiring user involvement. Some mentioned AI-driven protection, automatic updates, and smart authentication that adjusts based on user behaviour. These ideas demonstrate a clear preference for intelligent, hands-off solutions, such as background security and automated monitoring systems, that enhance safety without hindering productivity.
- **Usability:** Many participants emphasised the need to make cybersecurity more user-friendly and less disruptive. They preferred simple login methods such as one-click MFA, single sign-on (SSO), or passwordless authentication using biometrics or digital identity wallets. Others mentioned that frequent logins, long updates, and complex passwords reduce productivity. People also want more precise explanations of why security measures are necessary and easy-to-understand visual cues, such as lock icons, to indicate when something is secure. Suggestions included improving facial recognition in poor lighting (e.g., at night to recognise a face for login), reducing password changes, and using systems like YubiKeys or universal digital IDs. Overall, users want security that feels seamless, fast, and convenient.
- **Collaboration:** Some responses highlighted the importance of teamwork, awareness, and communication in cybersecurity. People mentioned that training should be engaging, varied, and relevant to different types of work. Others believed that security teams should act as service providers, supporting users, rather than as barriers to productivity. There were also calls for clearer explanations of why certain security measures exist, so employees can better understand and accept them. A few mentioned that discussions with colleagues help find practical solutions, and that systems should support users rather than create panic or frustration. In short, collaboration between users and cybersecurity professionals is crucial to establishing a balanced and supportive security culture.

4 Summary and observations

The key summary and observations regarding human-centric cybersecurity are as follows:

- The trend in human-centric research over a decade from 2015 to 2025 shows a clear trend of growth in human-centric research publications over time, peaking in 2024, when the highest number of studies was recorded.
- Most of the human-centric research is at the conceptual as well as experimental level, indicating a blend of theoretical and applied research.
- Most of the human-centric research focuses on developing structured, strategic approaches that integrate human factors into cybersecurity practices using advanced technologies like cryptography, and behaviour analytics across sectors such as education, government, health, software, smart home and communication networks.
- Human-centric research focuses more on the human psychological and cognitive factors, along with the working culture. These factors are related to both the designers and users of the systems.
- Most of the tools or technologies or models used in this research are cryptography, Structural Equational Modelling (SEM), Technical Formal Informal (TFI) model, Thematic analysis, multiple linear regression, attack tree analysis, Isabelle insider, and AI/ML.
- The results from the survey show that frequent password resets and frequent authentication are the most annoying cybersecurity measures. Additionally, most respondents consider biometric login the most user-friendly security feature, followed by single sign-on and automatic security patch updates.

5 Future directions

While this paper was primarily focused on academic discourse surrounding human-centric cybersecurity, as well as existing user-friendly security features and their mapping within the suggested

framework. It did not consider alternative approaches to minimising the dilemma between security and convenience, as well as immediateness.

One of these alternative approaches is reframing the dilemma entirely, that is, creating circumstances in which security and usability of a product, service, or tool are intrinsically intertwined and mutually determine each other. In that case, security is not perceived as a cumbersome add-on, but as an imperative and indispensable requirement for the product, service, or tool to work and fulfil its purpose.

It would entail pushing the Security by Design model to its fullest extent. The model describes a proactive approach to cybersecurity that integrates security systems from the initial stages to final deployment (CISA, 2023). It usually refers to digital products automatically, including built-in security features like MFA. In that case, however, the security feature is still perceived as an entity separate from the product itself. Full human-centrism of the cybersecurity feature would, however, require the security feature itself to be fully synchronised with the product.

To exemplify this level of maximal synchronisation, one can consider a physical safety analogy. Think of a car. Allowing for cultural nuances, think of a central European driver. The driver is most likely wearing a seat belt while driving. He/She does not perceive the act of putting on his seat belt as inducing a time delay to his drive. Instead, the two acts are so deeply intrinsically tied that the drive cannot be imagined without the seat belt.

Cybersecurity features - just like the safety function of a seat belt - can be framed similarly. If providing your password as a means of authentication does not delay your work but is an intrinsic part of it, we entirely circumvent the feeling that it's a burden.

Furthermore, psychological and behavioural research could provide deeper insights into how users internalise security behaviours once they become habitual and embedded in everyday workflows. Habit formation, cognitive load, trust calibration, and mental models of technology all shape whether users consider a security action as "part of the task" or as a separate, effortful step. Understanding these mechanisms would support the design of systems in which secure behaviour is not only automated or encouraged, but also intuitive, effortless, and self-reinforcing over time.

Similarly, the extent to which a cybersecurity feature is perceived as a burden is very much contextual. Further research could examine which contextual factors lead to cybersecurity being perceived as annoying. These contextual factors could span a variety of organisational, technological and individual dimensions, including workload pressures, interface design quality, organisational culture, and users' prior experiences with security technologies, as well as cultural background, gender, and other personal characteristics.

Carefully conducted to avoid any potential bias and false deductions, such as a study could not only demonstrate which elements of cybersecurity are perceived as annoying for what exact reasons and by whom, but also allow for a proactive stance on cybersecurity. A forward-looking cybersecurity posture derived therefrom would enable individualised, targeted cybersecurity measures, avoiding a one-size-fits-all approach. Effective cybersecurity would imply individually targeted cybersecurity.

Looking at contextuality, another broader socio-economic perspective on the question of human-centrism in cybersecurity arises: how does cybersecurity interact with larger ecosystems such as national law, regulatory frameworks, corporate norms, and the different stakeholders operating within them? Human-centrism cannot be realised in isolation, and the human is not a one-dimensional notion.

A strong consensus across groups emerged in our study regarding frictionless authentication. However, these preferred invisible or near-invisible security layers, such as biometrics and systems that continuously validate identity without explicit user actions, need to be contextualised as well. If the human does not consciously interact with technology but merges with it, how does that change the human-techno relation at large? What risks does it pose to its beholder, if a biometric factor is the authenticator and not a de-humanised combination of characters and numbers?

Finally, ethics- and trust-centric design could be further explored. Human-centrism does not start or end with non-disturbance; it also entails ethical considerations, inclusivity in who the cybersecurity framework applies to, and transparency, amongst others.

6 Conclusion

Humans play a significant role in cybersecurity research, whether as system designers, developers, testers, or regular users. This research concludes that most current studies are conceptual and experimental indicating a mature blend of theoretical and applied research. These studies focus on integrating psychological, cognitive, and cultural human factors into cybersecurity practices across sectors such as education, government, health, software, smart home networks. Commonly used tools include cryptography, Structural Equation Modelling (SEM), Technical Formal-Informal (TFI), thematic analysis, and AI/ML. Findings show that frequent password resets and repeated authentication frustrate users, while biometric logins, single sign-on, and automatic updates are seen as the most user-friendly security measures. The proposed framework provides a holistic and practically applicable foundation for human-centric cybersecurity by positioning people, processes, and technology as mutually reinforcing contributors to long-term resilience and sustainability.

Author contributions

RKo: Writing – review & editing, Writing – original draft, Visualization, Software, Formal analysis, Methodology, Conceptualization, Validation, Investigation. RKA: Writing – original draft, Funding acquisition, Resources, Project administration, Supervision, Writing – review & editing. AW: Methodology, Investigation, Writing – review & editing, Conceptualization, Writing – original draft.

Funding

The author(s) declared that financial support was received for this work and/or its publication. This work has been carried out within the framework, "AI Factory" at LTU.

Acknowledgments

We also acknowledge the valuable support and resources provided by the eMaintenanceLAB and two research centres, "Center for Intelligent Asset Management" (CIAM) and "Luleå Railway Research

Center - Järnvägstekniskt centrum” (JVTC), in conducting this research.

Conflict of interest

AW was employed by Cybersecurity Redefined.

The remaining author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that Generative AI was not used in the creation of this manuscript.

References

- Abdallah, M., Woods, D., and Cason, T. (2025). Selfish or malicious: price of malice in human-centric security decision-making for attack graph-based interdependent systems. *Int. J. Inf. Secur.* 25:4. doi: 10.1007/s10207-025-01180-3
- Al Ansari, M. J., Al Ahmed, Y., and El Bahnaswi, H. H. (2024). Balancing usability and protection in AI and data security: a human-centric approach. *International Conference on Software Defined Systems (SDS)*, 80–88. doi: 10.1109/SDS64317.2024.10883898
- Alemerien, K. (2017). User-friendly security patterns for designing social network websites. *Int. J. Technol. Hum. Interact.* 13, 39–60. doi: 10.4018/IJTHL.2017010103
- Ayodele, G. T., Abdulrahman, I. A., Alebiosu, J., Egbedion, G. E., and Akinbolajo, O. E. (2025). Human-centric cybersecurity: addressing the human factor in cyber defense strategies. *Iconic Research And Engineering Journals*, 8, 1488–1501.
- Beerman, J., Berent, D., Falter, Z., and Bhunia, S. (2023). “A review of colonial pipeline ransomware attack” in 2023 IEEE/ACM 23rd international symposium on cluster, cloud and internet computing workshops (CCGridW):IEEE, 8–15.
- Boer, H., and Seydel, E. R. (1996). “Protection motivation theory” in *Predicting health behaviour: Research and practice with social cognition models*. eds. M. Conner and P. Norman (Open University Press), 95–120.
- Breque, M., De Nul, L., and Petridis, A. (2021). Industry 5.0: towards a sustainable, human-centric and resilient European industry (No. KI-BD-20-021-EN-N). Directorate General for Research and Innovation (DG RTD) of the European Commission. doi: 10.2777/308407
- Bush, M., and Mashatan, A. (2025). “Bringing security home: the need for a human-centric approach to securing smart homes” in *The security of self: A human-centric approach to cybersecurity*. Canada: University of Ottawa Press.
- CISA. (2023). Secure by Design. Available online at: <https://www.cisa.gov/secure-by-design> (Accessed November 1, 2025).
- CNN. (2022). More than 8 million Cash App Investing customers potentially impacted by data breach linked to former employee. Available online at: <https://edition.cnn.com/2022/04/07/tech/cash-app-investing-breach> (Accessed November 1, 2025).
- Coffey, J. W., Haveard, M., and Golding, G. (2018). A case study in the implementation of a human-centric higher education cybersecurity program. *J. Cybersecur. Educ. Res. Pract.* 2018:4. doi: 10.62915/2472-2707.1028
- Deci, E. L., and Ryan, R. M. (1980). Self-determination theory: when mind mediates behavior. *J. Mind Behav.* 1, 33–43.
- Deibert, R. J. (2018). Toward a human-centric approach to cybersecurity. *Ethics Int. Aff.* 32, 411–424. doi: 10.1017/s0892679418000618
- Depassier, V., and Torres, R. (2018). A human-centric cyber security training tool for prioritizing MSNAs. In 2023 38th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW) (pp. 54–61). IEEE.
- Dikito, A. R., and Kaiser, M. S. (2023). The relationship between human-centric cybersecurity and cybercrime. *J. Inf. Technol.* 11, 58–66. doi: 10.59185/cd2a2q06
- DTEX. (2025). Cost of insider risks. Available online at: https://www2.dtexsystems.com/1/464342/2025-02-19/583csx/464342/1740000012hNhGjMpn/2025_Cost_of_Insider_Risks_Global_Report_by_Ponemon_and_DTEX.pdf
- Duncan, A. J., Creese, S., and Goldsmith, M. (2012). Insider attacks in cloud computing. *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (UK: Liverpool), 857–862.
- Gavaza, B., and Katsande, C. (2023). “A human-centric cybersecurity framework for ensuring cybersecurity readiness in universities” in *Effective cybersecurity operations for Enterprise-wide systems* (UK: IGI Global), 242–276.
- Gjertsås, K. R. (2024). Human-centric security: Integrating self-determination theory into organizational security practices. Norway: Norwegian University of Science and Technology.
- Gooch, B. (2025). The Louvre’s obvious password revealed after security criticised. Available online at: <https://www.independent.co.uk/bulletin/news/louvre-password-heist-security-video-b2860730.html> (Accessed November 20, 2025).
- Gopireddy, R. R. (2022). Human-centric cybersecurity: addressing the human element in cyber defense and ethical considerations in cybersecurity. *J. Artificial Intellig. Cloud Computing* 1, 1–5. doi: 10.47363/JAICC/2022(1)E118
- Grobler, M., Gaire, R., and Nepal, S. (2021). User, usage and usability: redefining human centric cyber security. *Front. Big Data* 4:583723. doi: 10.3389/fdata.2021.583723
- Hadi, A. (2023). User-friendly cybersecurity: A review of integrating usability and cognitive cost in SSDLC. University of South-Eastern Norway.
- Hakimi, M., Quchi, M. M., and Fazil, A. W. (2024). Human factors in cybersecurity: an in depth analysis of user centric studies. *Jurnal Ilmiah Multidisiplin Indonesia* 3, 20–33. doi: 10.58471/esaprom.v3i01.3832
- Hilowle, M., Yeoh, W., Grobler, M., Pye, G., and Jiang, F. (2023). Users’ adoption of national digital identity systems: human-centric cybersecurity review. *J. Comput. Inf. Syst.* 63, 1264–1279. doi: 10.1080/08874417.2022.2140089
- Hilowle, M., Yeoh, W., Grobler, M., Pye, G., and Jiang, F. (2024). Improving national digital identity systems usage: human-centric cybersecurity survey. *J. Comput. Inf. Syst.* 64, 820–834. doi: 10.1080/08874417.2023.2251452
- Hussain, Z. (2017). A user friendly security framework for the protection of confidential information. Available online at: <https://www.researchgate.net/publication/317040838> (Accessed November 20, 2025).
- Jamil, H., Zia, T., Nayeem, T., Whitty, M. T., and D’Alessandro, S. (2025). Human-centric cyber security: applying protection motivation theory to analyse micro business owners’ security behaviours. *Inf. Comput. Secur.* 33, 49–76. doi: 10.1108/ICS-10-2023-0176
- Jethava, G., Shukla, N., Chauhan, D., and Patel, K. (2025). Defending the digital frontier: a user-friendly cybersecurity toolkit. *Proceedings of International Conference on Computational Intelligence and Data Engineering: ICCIDE 2024*, (Singapore: Springer Nature Singapore), 243.
- Kammüller, F. (2018). Human centric security and privacy for the IoT using formal techniques. London, UK.
- Kammüller, F., Augusto, J. C., and Jones, S. (2017). “Security and privacy requirements engineering for human centric IoT systems using eFRIEND and Isabelle” in *In 2017 IEEE 15th international conference on software engineering research, management and applications (SERA)* (UK: IEEE), 401–406.
- Kassicieh, S., Lipinski, V., and Seazzu, A. F. (2015). Human centric cyber security: what are the new trends in data protection? *Portland Int. Conf. Manag. Eng. Technol.* 2015, 1321–1338. doi: 10.1109/PICMET.2015.7273084
- Kelechukwu, O., Ngugi, J., and Sumbiri, D. (2025). Human-centric cybersecurity training: examining the effectiveness of human-centric approaches to cybersecurity training compared to traditional methods, focusing on behavior change. *J. Information Technol.* 5, 51–68. doi: 10.70619/vol5iss12pp51-68-697

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher’s note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

- Khadka, K., and Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *Int. J. Inf. Secur.* 24, 1–13. doi: 10.1007/s10207-025-01032-0
- Kioskli, K., Fotis, T., Nifakos, S., and Mouratidis, H. (2023). The importance of Conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. *Applied Sci.* 13:3410. doi: 10.3390/app13063410
- Klein, J., and Hossain, K. (2020). Conceptualising human-centric cyber security in the Arctic in light of digitalisation and climate change. *Arctic Review Law Politics* 11, 1–18. doi: 10.2307/48710620
- Kurdi, M. H., Denden, M., and Paul, D. (2024). A study on the challenges of human-centric cyber-security and the guarantee of information quality. *J. Inf. Secur.* 15, 218–231. doi: 10.4236/jis.2024.152013
- Lakshmisree, C. S. (2016). A biometrics based user-centric authentication approach for user friendly security system *IJARBEST* 2, 885–895.
- Leavitt, H. J. (1964). *Applied organization change in industry: Structural*. And: Technical.
- Magramo, K. (2024). *British engineering giant Arup revealed as 25 million deepfake scam victim*. Atlanta, GA, USA: CNN Business May, 17.
- Marino, V. (2023). User-friendly security automation for Domotic networks. (Doctoral dissertation, Politecnico di Torino).
- Mohammed, S. A. (2025). Human-centric cybersecurity: addressing insider threats with behavior analytics. *Archiv.* 104–113. doi: 10.25215/9371838892.12
- Moher, D., Liberati, A., Tetzlaff, J., and Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *BMJ* 339. doi: 10.1136/bmj.b2535
- Mohurle, S., and Patil, M. (2017). A brief study of wannacry threat: ransomware attack 2017. *Int. J. Adv. Res. Comput. Sci.* 8, 1938–1940.
- Morgan, P. L., Asquith, P. M., Bishop, L. M., Raywood-Burke, G., Wedgbury, A., and Jones, K. (2020). A new hope: human-centric cybersecurity research embedded within organizations. *International Conference on Human-Computer Interaction*, 206–216. doi: 10.1007/978-3-030-50309-3_14
- Muhudin Hilowle, M. (2023). *National Digital Identity Systems: A perspective of human-centric National Digital Identity Systems: A perspective of human-centric cybersecurity* AUTHOR(S), vol. 64, 820–834 doi: 10.1080/08874417.2023.2251452.
- Narayanan, A., and Srinivasan, S. (2025). “Human-centric cybersecurity methods in financial services: employ behavioral analytics in the face of credential theft, phishing, and social engineering” in 2025 IEEE 5th international conference on ICT in business industry & government (Indore, India: ICTBIG), 1–7.
- Ozkan Ozen, Y. D., Ozbiltekin Pala, M., and Ayranci, G. (2024). Evaluating human-centric cyber security risks in the manufacturing industry. *Int. J. Manuf. Res.* 19, 322–337. doi: 10.1504/ijmr.2024.10068139
- Paljug, K., and Mikac, R. (2020). Contemporary crises: Case study of UBER. *Contemporary Macedonian Defence/Sovremena Makedonska Odbrana*, 20, 93–106.
- Ra, G., Kim, T., and Lee, I. (2021). VAIM: verifiable anonymous identity Management for Human-Centric Security and Privacy in the internet of things. *IEEE Access* 9, 75945–75960. doi: 10.1109/ACCESS.2021.3080329
- Rahman, T., Rohan, R., Pal, D., and Kanthamanon, P. (2021). “Human factors in cybersecurity: a scoping review” in Proceedings of the 12th international conference on advances in information technology. (United States: Association of Computing Machinery New York), 1–11.
- Rao, Z. F. (2024). Human-centric cybersecurity: Safeguarding individuals in the digital age. Scotland (Master thesis): University of Glasgow.
- Rishiwal, V., Agarwal, U., Alotaibi, A., Tanwar, S., Yadav, P., and Yadav, M. (2024). Exploring secure V2X communication networks for human-centric security and privacy in smart cities. *IEEE Access* 12, 138763–138788. doi: 10.1109/ACCESS.2024.3467002
- Rohan, R., Funilkul, S., Pal, D., and Thapliyal, H. (2021). Humans in the loop: cyber-security aspects in the consumer IoT context. *IEEE Consumer Electronics Magazine* 11, 78–84. doi: 10.1109/MCE.2021.3095385
- Rothenberg, E. (2023). CNN. Tesla begins notifying workers who were affected by data breach. Available online at: <https://edition.cnn.com/2023/08/19/business/tesla-data-breach-employee-personal-info> (Accessed October 10, 2025).
- Ryan, P. Y. A. (2025). Designing Human-centric security protocols. In: Morogan, L., Roenne, P., Bica, I. (eds) *Innovative Security Solutions for Information Technology and Communications. SecITC 2024. Lecture Notes in Computer Science*. (Cham: Springer), 15595. doi: 10.1007/978-3-031-87760-5_1
- Salinas. (2025). Case No. 22-cv-04823. District Court for the Northern District of California. Available online at: <https://cashappsecuritysettlement.com/> (Accessed December 1, 2025).
- Schneier, B. (2015). *Secrets and lies: Digital security in a networked world*. USA: John Wiley & Sons.
- Tabari, A. Z. (2021). Human-centric cybersecurity research: from trapping the bad guys to helping the good ones (Doctoral dissertation, University of South Florida). Available online at: <https://digitalcommons.usf.edu/etd> (Accessed November 20, 2025).
- Tambe-Jagtap, S. N. (2023). Human-centric cybersecurity: understanding and mitigating the role of human error in cyber incidents. *SHIFRA* 2023, 53–59. doi: 10.70470/shifra/2023/007
- Tamzid. (2025). 250+ Cybercrime Statistics for 2025. Available online at: <https://www.brightdefense.com/resources/cybercrime-statistics/#pp-toc-nd0c5lfqet8g-anchor-9>
- Tari, Z., and Mahmud, R. (2025). Augmenting digital ecosystem resilience through human-centric cybersecurity solutions. *IEEE Trans. Eng. Manag.* 72, 3892–3908. doi: 10.1109/TEM.2025.3606637
- Troublefield, T. C. (2025). The Cyberpsychology of small and medium-sized enterprises cybersecurity: a human-centric approach to policy development. *J. Inf. Secur.* 16, 158–183. doi: 10.4236/jis.2025.161009
- van der Kleij, R., Van Hemert, D., Te Paske, B. J., and Rooijackers, T. (2024). Human-centric security engineering: towards a research agenda. *Hum. Factors Des. Eng. Comput* 159, 8–10. doi: 10.54941/ahfe1005596
- Wang, L. (2024). “Investigation on human-centric security based on understanding the role of user behavior in information security” in 2024 international conference on electronics and devices, computational science (ICEDCS), 1115–1122. IEEE.
- Zhou, S., and Wang, Y. (2025). Build a human-centric maritime transportation cybersecurity protection system based on MARITIME. *International Journal of Advanced AI Applications* 1, 1–28.