CHAPTER _

Future Directions in Human-Centred Cybersecurity

Animesh Kairi[1]*, Tapas Bhadra[2], Priyanka Das[3]

[1]Department of Computer Science and Engineering, Institute of Engineering & Management, Kolkata, West Bengal, India.
[2]Department of Computer Science and Engineering, Aliah University, Kolkata, West Bengal, India.
[3]Department of Computer Application, Institute of Engineering & Management, Kolkata, West Bengal, India.

E-mail: ani.kairi@gmail.com,tapas.bhadra@aliah.ac.in,priyanka.das@iem.edu.in*

Abstract: There is a new concept of human-centered cybersecurity (HCC), (also known as usable security) that is increasingly becoming the foundation of protecting complex digital environments. With the changing technology, cyber security issues are becoming more interdependent with human behavior, organizational culture, and the socio-technical systems. This chapter analyses the future perspective of HCC with focus on three pillars on which the organization rests and that are trust, transparency and resiliency. It is an amalgamation of the best practices of major standards organizations like NIST and ISO, government agencies like CISA, and the recent scholarly literature about the human factor, artificially intelligent threats, and software supply-chain vulnerabilities. The chapter examines the impact of new technologies, such as artificial intelligence, post-quantum cryptography, and software transparency models, to change the concept of security and provoke new challenges to be used. Social engineering through artificial intelligence, the emergence of deep fakes, and automatic attacks require flexible defense based on the integration of explainable AIs and user-friendly verification processes. In the same vein, post-quantum or cryptography should be transitioned to carefully in order to make sure it is operational and disrupt operations less. Software Bills of Materials (SBOMs) and vulnerability attestations are identified as key providers of supply-chain security, although they need to be provided in human-read formats to enable informed decision-making. In addition to technology, the chapter also gives relevance to the role played by behavioral science and inclusive design in promoting sustainable security practices. It ends with a research agenda to fill in gaps in longitudinal behavior change, accessibility, and collaboration between humans and AI and makes HCC a pivotal facilitator of cybersecurity in the decade ahead.

Keywords: Human-centred Cybersecurity, Usability security and Privacy, Human-computer interaction(HCI),User behaviour and security awareness, Cognitive factors in cybersecurity, Social engineering defence, Security by design, Privacy- preserving systems, Explainable AI security, Adaptive authentication system, Insider threat control systems, Socio-technical security, Human-in-the-loop security, Behavioural biometrics, Cybersecurity education and training, Inclusive and accessible security, Futuristic control of cyber risk, AI-driven user-centric.

1. INTRODUCTION: WHY "HUMAN-CENTERED" NOW?

People are as important as technology in cyberspace when it comes to cybersecurity results. The Federal Cybersecurity R&D Strategic Plan of the U.S. National Science and Technology Council puts human centered cybersecurity at the forefront and states that the system design should take into consideration what the end users need, value and can actually do, and usability, inclusiveness and user experience should all be considered aspects of system security effectiveness and not as an afterthought [1][2]. This focus was formalized by NIST, which changed the title of its Human Centered Cybersecurity program and broadened its attention to encompass social, organizational as well as psychological aspects of adoption and behavior. The stakes are quite basic: according to industry research, a significant percentage of breaches has to be attributed to the human factor- flawed decisions, configuration mistakes, and social engineering [3][4]. HCC research records that a consistent gap exists between theoretical understanding and practice, whereby practitioners are keen to embrace guidance but have problems assimilating it. CISA defines resilience as a priority on national level: the capability to prepare, adapt, withstand, and swiftly recover in the event of disruption in the critical infrastructure and supply chains.

The chapter claims that cybersecurity will be won (or lost) at the border between complex systems and human judgment of decisions [5]. It establishes guidelines on integrating trust, transparency, and resiliency using human centric design, governance, and technology.

2. CONCEPTUAL FOUNDATIONS

2.1 From "Usable Security" to Human-Centered Cybersecurity

Traditionally, the concept of usable security developed into human centered cybersecurity. Usable security traditionally involved making security work user-friendly (e.g., authentication) [6]. However, HCC in the modern day extends the use of the approach to people-process and technology relations, and seeks to make the safe path the effortless one, and recovery amnesties [7]. The HCC program, developed by NIST, defines this change and provides evidence-based instructions that can enable individuals

to be active participants in cybersecurity. A more recent survey recasts the three key elements of HCC as the 3Us, including user, usage and usability, which proposed a paradigm shift in thinking away functional, usage centered security, toward user centered security which is responsive to human constraints and context [8].

2.2 Human-Centered Design Standards

Human centred design (HCD) is codified by ISO 9241 210 as life cycle: express appreciation of users and situations, of creative design, involvement of users in the entire process, and multidisciplinary teams. These postulates, but not security specific, directly translate in creating secure systems which can be operationally utilized by humans without making mistakes [9]. In 2025, the 2019 edition was established as a current one. The practical advice PMaps HCD with security/privacy, such as how to elicit mental models, personas, and privacy requirements [10], the former work better than costly workarounds to adopt.

2.3 Trust Architecture: Privacy by Design (PbD)

One of the ways that privacy is used to establish trust is through the privacy by design framework [11], which establishes seven cornerstones, including: proactive protection, privacy as default, end to end security, and visibility/ transparency. PbD has come to reflect in a number of regulatory regimes (e.g. the GDPR's data protection by design), although it is most useful when combined with both HCD and usability such that users are able and willing to perform privacy preserving behaviours. Opponents of the vagueness of PbD have driven actual mappings of fair information practices and implementation checklists [12].

3. NEW MENACE ON THE HORIZON AND THE HUMAN FACTOR

3.1 AI Initiated Social Engineering

Deepfakes (voice/video) are increased through generative AI and used to commit phishing, vishing, and impersonation. In 2024-2025, reports and analyses cite acute increases in social engineering purpose by AI and the challenge that even people cannot easily spot them without the added verification MFA, out of band checks [13]. The industry projections are that SOC operations will have a metamorphosis of agentic automation, although it also points out that there are shortcomings in workforce readiness, creating the necessity of AI proficiency among workers [14].

3.2 Behavioral Weaknesses: What the Research Shows

Bibliometric statements and systematic review literature point to psychological reasons (cognitive biases, self-efficacy, cues to action) and the weaknesses of generic awareness trainings. There is some evidence that behaviourally informed interventions (nudges, gamification, and realistic simulations) are more successful than one size fits all interventions. Recent studies using Health Belief Model to phishing depict perceived severity, importance and self-efficacy predicting protective behaviour: perceived susceptibility alone is a weak predictor-implications to curriculum design and communication [15]. There is an interdisciplinary survey that suggests frameworks that integrate psychological resilience, adaptive training, and ethical AI governance to improve the existence of socio technical disconnections.

3.3 Supply Chain and Transparency Risks

The definition of transparency is shifting towards openness of software. Software Bill of Materials (SBOM) has become a proposed block of building supply chain security, and CISA has a range of guidance and minimum expectations (2024 framing; 2025 draft upgrades). Comparative analyses demonstrate the development of minimum elements e.g. explicit authorship, component hashes, license data, generation context which are intended to scale operationalize SBOM. According to practitioner resources, SBOMs aid in defining the vulnerability exposure and license concerns to enhance risk management in the contemporary ecosystems [3].

3.4 Quantum Migration of risk and Cryptography

The introduction of post quantum cryptography (PQC) entails instant human level and organizational feedback: cataloguing crypto utilization, migration scheduling, and backwards compatibility of the solution. NIST has approved three PQC standards (a fourth is in progress) in 2024, calling on early migration towards its ability to obstruct data endurance on a long-stored basis against "harvest now, decrypt later" (and protect). A migration in stages, application layer audits, and governing have been highlighted as part of the strategic direction to support the most intricate crypto migration in cybersecurity history [2].

4. PRINCIPLES AND PATTERNS DESIGNING TO BE TRUSTED

4.1 Trust as a Culmination of Experience

Security builds credibility in predictable and explainable and recoverable interactions. There is an affinity between HCD and PbD in case systems:

i. Reduce the unexpected (predictability),
ii. Expose security state to visibility (transparency), and
iii. Support remedial recovery (resilience). Standards and programmatic direction focuses on solution design that is both practical and not just theoretical and on empowering the users as partners.

4.2 Secure by Design versus Human by Design

The advisory bodies established by CISA and community capacity building resilience programs require the adoption of secure by design in the critical sectors, connecting it to the governance and contingency planning. Such attempts focus on third party risk, techniques of living off the land, and scenario exercises that challenge human systems as well as technical systems communication and coordination [1].

4.3 Futures Authentication: Friction and Passkeys

Authentication without a password (e.g. FIDO passkeys) is claimed to be less cognitive cytotoxic and more phishing resistant. Although the measures of adoption are dynamic, the human imperative of the problem is evident: minimize user friction, but maintain the transparency of risk and avoid an availability of a fallback when offering a way to fall back is essential, without issuing new weak links. About the actual adoption research, organizations are advised to monitor antithetical FIDO and platform reports.

4.4 Zero Trust with a Human Lens

Zero Trust Architecture (ZTA) has been referred to as a technical paradigm, but its effectiveness hinges on human centric policy, experience design and explainability: users have to know why access has been denied, how to fix the posture and what indicators are important. NIST SP 800 207 describes zero trust in terms of unremitting verification and least privilege; UX patterns to allow consent, posture remediation and exception management should be added to future practice to minimize shadow IT practices. Modular architecture in reasonable sensor frameworks (Policy Engine, Administrator, and Enforcement Point) is provided by practitioner guides and sector articles, which may be exposed via unambiguous, human-companionable user messaging and self-service remediation.

5. TRANSPARENCY AT SCALE: SBOMS, EXPLAINABILITY AND UX

5.1 SBOM as an Everyday Artifact

The systems of the future will not be using SBOMs as compliance documents but instead have them installed as a part of update workflows and vulnerability dashboards as

well as procurement. SBOM resources and framing documents of CISA offer minimum requirements and defines and community activities go further with formats (SPDX, CycloneDX) and automation. In the 2025 draft, properties such as component hashes, and the generation context are raised in ranking the provenance and machine processing -a vital requirement in user facing risk communication [15].

5.2 Human Readable Risk Signals

The lack of transparency is present when the signals are not understandable. The data of SBOM in the future should be converted into human readable risk stories: the component in question, the exploitability, the affected persons, and actions to take next. This is expected by the concept of the Vulnerability Exploitability eXchange (VEX), where the attestation status of vulnerabilities, which are known to impact a product, is indicated; matching VEX with UX policies may alleviate alert fatigue.

6. RESILIENCE: TRAINING AND ORGANIZING PEOPLE AND ORGANIZATIONS

6.1 Resilience Services and Governance

In CISA Resilience Services, the definition of resilience is the capacity to prepare, adapt, withstand and recover, which is executed in terms of assessments, planning advice and alliances. New Cybersecurity Performance Goals (CPG) are based on NIST CSF 2.0 and includes a Govern function which increases leadership responsibility and incident communication important accountable components of resilience [13].

6.2 NIST CSF 2.0: Human Centered Outcomes

The outcome taxonomy of CSF 2.0 (2024) by NIST is intended to be used only by boards, legal, HR, and technical stakeholders: the CSF 2.0 to the category of Identify/Protect/Detect/Respond/Recover is explicit about who action is aimed at: human. The integration of the CSF outcomes into the performance reviews, budgetary, and training systems helps make resilience an organizational behavior, rather than a tooling [14].

6.3 Well Being and Incident Culture amongst the workforce

The need to combat human stress, burnout and mental load during an incident is the main requirement of resilience. The reports on the advisory committees focus on scenario planning and resource gaps filling of smaller organizations -human capacity as resiliency dependency. Future directions are to incorporate the principles of psychological safety and debrief rituals in the IR plans and grow in line with the HCD principles (iterative learning with stakeholders).

7. AI: GUARDRAILS, FLUENCY, AND AGENTIC OPERATIONS

7.1 AI Governance Meets HCC

Businesses should find a middle ground between the two aspects of AI, as an amplifier of attacks and as a defense accelerator. The 2026 tech trends of Deloitte identify shadow AI and governance gap to recommend specific frameworks, which supplement the traditional security principles with AI-specific ones (data provenance, model integrity, agent permissions). The Google Cloud 2026 projections focus on security automation and caution that organizations have not trained workforces to be safe using AI-a human centered training gap.

7.2 Smart AI UX: security

The next generation SOCs will have explainable AI interfaces, which indicate why a particular model flagged or performed a specific action, and operators would be able to calibrate trust. The AI fluency of all employees who work with agentic tools should be trained (prompts, failure modes, adversarial risks) and not just security teams.

8. RESEARCH AGENDA: WHAT WE STILL DON'T KNOW

i. **Open-ended Behavior Change -** Which game combinations of nudges, training, and redesigning of the interface can maintain protective behaviors more than short intervention campaigns? The evidence of bibliometry hints psychological constructs are important, yet limited number of controlled, multi years, research in different populations.

ii. **Inclusive Security and Accessibility -** All Hamilton-Burrini are welcome to the tango! Inclusive design is encouraged by ISO 9241 210, and HCC should do more efforts to serve underserved situations, generational differences, and accessibility security trade-offs.

iii. **Human Centered Zero Trust Patterns -** We do not have standard UX patterns to posture remediation, exception requests, and just in time least privilege that would minimize frustration and shadow IT.

iv. **SBOM Supportive and analysis of information -** Determining effective methodologies for translating intricate SBOM and VEX datasets into comprehensible, actionable intelligence for non-specialist stakeholders remains a critical research challenge. Current literature reveals a paucity of empirical studies evaluating the usability and decision-support capabilities of SBOM dashboards within human-centered cybersecurity frameworks.

9. PRACTICE FRAMEWORK: THE TTR (TRUST-TRANSPARENCY-RESILIENCE) PLAYBOOK

9.1 Trust

i. **Safer than safe authentication -** Use phishing resistant MFA/passkeys; offer recoverability/diffuse user experiences, continuous testing of user experience to prevent the use of shadow credentials.

ii. **Privacy by Design questionnaires -** Integrate PbD principles into design reviews: default privacy, data minimization, end to end lifecycle protection, and auditability**.**

iii. **Explainable policies -** Indicate the presence of access decision and the steps to be taken to correct it to enhance credibility and minimize support tickets (Map to SP 800 207 policy components).

9.2 Transparency

i. **SBOM everywhere** - Mandate SBOMs of the suppliers; commit VEX to vulnerability processes; make risk narratives available in human readable formats in dashboards.

ii. **Human centered alerts -** Make high impact, low volume alerts, where the action is easy to take, their priority; probabilistic deepfakes detections, without the ability to validate identity with determinism, should not be a priority.

iii. **Metrics that matter** - Monitor security notices understanding and effective self remediation rates- more than technical MTTR- to 2.0 outcomes of CSF.

9.3 Resilience

i. **Governance first -** Embark on Govern of the CPG 2.0; attributing explicit roles, put incident communications to test and publish the post mortem with learning outcomes.

ii. **Scenario exercises -** Conduct cross functional exercises dedicated to living off the land, third party outages, and deepfake impersonation of executives; evaluate human coordination and quality of the decisions.

iii. **Crypto transition program -** Planed PQC migration, provide inventory cryptography, and train developers of algorithm modifications and performance trade offs.

10. IMPROVE PREMIUM FUNCTIONALITY AND FOCUS ON THE MARKETPLACE

i. **Create an HCC Community of interest (COI) -** Connect researchers, practitioners, and educators using the model of NIST; Co create evidence based artifacts (patterns, curricula).
ii. **Baseline with NIST CSF 2.0 -** Establish a profile that focuses on human centric results (governance, communication, training efficacy); consistent with CPG 2.0.
iii. **Operate human centered Zero Trust pilots** - Begin with those applications that have a very high risk profile; create UX around access refusals and posture remediation; work on user feedback through the iterative process (ISO HCD).
iv. **Operationalize SBOM** - must have SBOMs procured; must use tools which create and use SBOMs; must adopt VEX; internal guidance published publicly to product teams.
v. **Artificial intelligence social engineering defense -** Introducing layers of identity verifications with communications platforms; conducting deepfake exercises; training AI in security awareness courses.
vi. **Plan PQC migration** - Develop a centric inventory based on applications, develop and test Kyber/Dilithium where possible, revise core management and protocols, communicate the changes to customers.

11. CASE ILLUSTRATIONS (CONDENSED)

i. **Smart-home ecosystems.** By focusing on the emotional and personal consequences of any breach (e.g., safety and privacy at home) and creating controls that users can influence, a human centered approach empowers the IoT security to become stronger, which is also becoming an emerging priority of the national applied research.
ii. **Critical infrastructure operators.** Use of CPG 2.0 with focus on governance, resilience testing and cross sector exercises is a solution to human coordination failures during nation state campaigns.

12. CONCLUSION: DESIGNING FOR PEOPLE, NOT JUST PERIMETERS

In conclusion, the idea is to design people and not merely perimeters. Transformation Human-centred cybersecurity (HCC) represents a shift back to a socio-technical science in which trust, transparency, and resilience are no longer the elements that make security a great idea but rather the fundamental design and governance priority. Contrary to the era of distributed ecosystems, AI-scenar attacks as well as sophisticated supply chains, traditional perimeter-based models are inadequate. The coming 10 years will require explainable Zero Trust architecture, AI fluent employees, and operational transparency via techniques such as Software Bills of Materials (SBOMs) and Vulnerability

Exploitability eXchange (VEX). Also, the transition to the post-quantum cryptography (PQC) will necessitate inclusive practices that focus on usability and reduce disruption. The creation of cybersecurity in the future needs to consider iterative, human designs principles as encompassed by ISO 9241-210 to make sure the systems are secure in practice, rather than theory. It consists of making security simple to use, regards privacy as a default, and designed recovery mechanisms that minimize the damage in case of errors. Cybersecurity Governance Frameworks including NISTs Cybersecurity Framework 2.0 and CISAs Cybersecurity Performance Goals are considered a base, and their effectiveness depends on cultural transference and workforce empowerment.

The threat will develop new technologies that will transform the risks and defenses. Automation represented by AI has the potential to reduce the period of holding onto potential indicators and launching the response, but lack of explainability and ethical bounds may destroy trust. Likewise, the transparency programs need to change and go beyond compliance docs to non-expert actionable information. The only thing that will make resilience will be based on incorporating psychological safety, adaptive training, and collaboration across sectors into the incident response planning. The operative imperative of educators, policymakers and practitioners is evident: make doing right easy, doing wrong hard, and recovering easy when it goes afoul--the culture of NIST program in HCC. Cybersecurity will be able to shift to proactive, inclusive and inclusive mode of resilience by focusing on human factors alongside technical innovation, to generate a partnership between cybersecurity and technical innovation enabling digital ecosystems to be considerate and responsive in an increasingly complex future.

CONFLICT OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this chapter.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to all individuals and institutions who contributed to the successful completion of this work. Special thanks are extended to colleagues, mentors, and reviewers for their valuable insights and constructive feedback. The authors also acknowledge the support of their respective institutions for providing the necessary resources and environment to carry out this research.

References

[1] National Institute of Standards and Technology. (2025, March 26). *Human-centered cybersecurity program overview*. NIST.

[2] Haney, J. M., & Jacobs, J. L. (2023, September 28). *NIST unveils newly named human-centered cybersecurity program*. National Institute of Standards and Technology.
[3] National Institute of Standards and Technology, Computer Security Resource Center. (2025, September 12). *Human-centered cybersecurity: About*. NIST CSRC.
[4] Haney, J. M., Jacobs, J. L., & Smith, M. (2024). *Integrating human-centered cybersecurity research into practice: Practitioner survey*. National Institute of Standards and Technology.
[5] Grobler, M., Flowerday, S., & von Solms, R. (2021). User, usage and usability: Redefining human-centric cyber security. *Frontiers in Big Data, 4*, Article 740734. https://doi.org/10.3389/fdata.2021.740734
[6] International Organization for Standardization. (2019). *ISO 9241-210:2019—Ergonomics of human-system interaction—Human-centred design for interactive systems* (Confirmed 2025). ISO.
[7] Groen, E. C., Kauer, M., Mayer, P., & Felderer, M. (2023). *Achieving usable security and privacy through human-centered design*. Springer.
[8] Cavoukian, A. (2010/2011). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.
[9] Cavoukian, A. (2012). *Privacy by design principles: Implementation and mapping to fair information practices*. University of Waterloo.
Wikipedia contributors. (2025). *Privacy by design*. Wikipedia.
[10] The Hacker News. (2025, May 13). Deepfake defense in the age of AI.
Forbes Technology Council. (2025, August 25). Deepfakes and social engineering: A growing threat. Forbes.
[11] CrowdStrike. (2025, May 6). AI-powered social engineering attacks.
Google Cloud. (2025, December 12). 2026 cybersecurity forecast: Agentic automation and AI fluency. Google Cloud Blog.
[12] Desolda, G., Ardito, C., & Matera, M. (2022). Human factors in phishing attacks: A systematic literature review. ACM Computing Surveys, 54(8), Article 169.
[13] Mutlutürk, M., Aydın, S., & Karabatak, M. (2024, October 15). Phishing and the human factor: A bibliometric analysis (2006–2024). Applied Sciences, 14(20), 9012. https://doi.org/10.3390/app14209012
[14] Gwenhure, Y. (2025, November 4). University students' security behavior versus phishing: A health belief model approach. Journal of Cybersecurity.
[15] Khadka, R., & Ullah, I. (2025, April 29). Human factors in cybersecurity: An interdisciplinary review and research framework. Springer Journal of Information Security.