What is Human-Centered Cybersecurity?

Julie M. Haney
National Institute of Standards and Technology

Julio Poveda
University of Maryland, College Park

Ozioma Okehielem
University of Maryland, Eastern Shore

Jody L. Jacobs
National Institute of Standards and Technology

Rosanna Guadagno
University of Oulu

Arun Vishwanath
Cyber Hygiene Academy

1 Introduction

The absence of a unified understanding regarding the human element in cybersecurity poses significant operational and strategic risks [2, 3]. Narrow perspectives—-such as reducing the space to compliance-based awareness training—-and contrasting views of general employees as organizational antagonists ("the weakest link") rather than protagonists ("capable partners") often result in misaligned policies and toxic cultures [2, 5, 16, 17]. Further, these inconsistencies can hinder interdisciplinary collaboration and collective knowledge sharing [4, 5, 12, 14].

To mitigate these gaps, the establishment of standardized terminology is critical. Standardized terms function as boundary objects: translational devices that facilitate common ground and collective responsibility between different communities, such as behavioral science and technical cybersecurity [8]. However, the human domain of cybersecurity suffers from a distinct lack of standardized vocabulary. While *human-centered cybersecurity* (HCC) is an emerging team across government [9, 10], academia [7, 15, 17], and industry [1, 13], practitioners often conflate HCC with narrower, distinct concepts like usability, security awareness, human error, and human risk management [2, 3, 11, 17].

As a first step towards developing a shared understanding, we engaged in mixed-methods research to discover how the cybersecurity community currently perceives HCC. We conducted an interview study (N = 40) and a survey study (N = 323) of individuals representing different stakeholder groups (those impacting and impacted by organizational cybersecurity programs). We report on preliminary results related to the following research questions:

RQ1: How do cybersecurity stakeholders describe human-centered cybersecurity?

RQ2: Who do stakeholders think are the "humans" referred to in the term human-centered cybersecurity?

This understanding can 1) inform future efforts towards developing standards on how we think about and address the human element of cybersecurity and 2) start to identify conflicting views needing to be addressed before realization of widespread HCC adoption.

2 Methodology

The research was approved by our institutional Research Protections Office, with all participants providing consent.

Interviews: We conducted virtual, semi-structured interviews with 40 participants to ask about their thoughts on HCC. We purposefully recruited via professional contacts and snowball sampling to ensure participants provided information-rich responses and represented a variety of stakeholder groups:

- *Decision Makers* (n = 7) who make strategic security/IT decisions or lead teams/organizations (e.g., CISO, security manager, senior executive)
- *Technical Professionals* (n = 7) who do hands-on security/IT work, create security products, or conduct technical research (e.g., security analyst, system administrator, developer, cybersecurity researcher)
- *Policy and Regulatory Professionals* (n = 5) who create, interpret, or enforce cybersecurity/IT rules, standards, or guidance (e.g., risk analyst, policy analyst, auditor, compliance manager, guidance developer)
- *Security communications and learning professionals* (n = 5) who create security training materials or communicate security information (e.g., training specialist, security awareness program manager)
- *Human Factors/Behavior Practitioners* (n = 9) who apply human-computer interaction, human factors, psychology, or related disciplines to organizational cybersecurity (e.g.,

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23-26, 2026, Hannover, Germany.

human factors engineer, user experience professional, cyberpsychologist)
- *Human Factors/Behavior Researchers* (n = 7) who research human factors, psychology, or related disciplines in the cybersecurity context (e.g., usable security researcher)

Four research team members conducted thematic analysis of the interview data, which involved iterative deductive and inductive coding to develop a codebook, discussion and resolution of coding conflicts, and memoing.

Survey: We also conducted an online, anonymous survey (N = 323). Participants described HCC in their own words in an open-ended question and indicated who they thought were the humans in cybersecurity in a multiple-select question.

We recruited organizational employees via professional contacts and cybersecurity mailing lists who self-categorized into one of the following stakeholder roles aligned with the interviews: Decision Makers (n = 67, 21%); Technical Professionals (n = 71, 22%); Policy and Regulatory Professionals (n = 74, 23%); Security communications and Learning Professionals (n = 38, 12%), and a Human Factors/Behavior Specialists group that combined practitioners and researchers (n = 43, 13%). We added a General End Users role (n = 30, 9%) to represent employees without specialized cybersecurity or IT expertise.

Two research team members used the interview codebook to independently code open-ended responses, then met to discuss and resolve coding conflicts. The interview and survey teams then collectively met to identify overarching themes present across both studies. We also calculated descriptive statistics to quantify the frequency with which each stakeholder group used the codes to describe HCC as well as who they identified as the humans in HCC.

3 Preliminary Results

3.1 RQ1: How is HCC described?

When first asked to describe HCC, a few participants framed it as generally addressing human factors, including application and understanding of human nature, psychology, needs, and cognition in the cybersecurity context. Most, however, provided descriptions that included the following concepts.

Human-system interactions. As the most prevalent theme across both studies, participants described HCC as including an understanding of people's behaviors and interactions with cybersecurity technologies, processes, and policies (i.e., sociotechnical systems) and how to design systems so they work with and not against people's abilities, limitations, and workflows. This perspective included concepts such as human-centered design, usability, and the facilitation of secure behaviors when people interact with systems.

Security culture. Culture encompasses the values, attitudes, and beliefs that drive behaviors in organizations [6]. Participants described a mindset shift from a focus on technological solutions to a people-centered perspective that permeates how organizations approach and prioritize cybersecurity. This includes creating an environment in which: employees feel motivated to be active participants in cybersecurity; leadership visibly demonstrates buy-in for cybersecurity; different groups within the organization work together to foster security; employees' feedback and needs are considered when making security decisions; and employees feel comfortable admitting mistakes and asking questions.

Human vulnerabilities. Some participants believed that HCC involved human errors and risks, including understanding and mitigating human vulnerabilities to social engineering, natural human limitations and flaws, and environmental factors that negatively impact people (e.g., stress, cognitive overload). While a number of survey participants used some version of the adage "humans are the weakest link" to categorize people as problematic in cybersecurity, interview participants generally pushed back against this negative characterization.

Knowledge, awareness, and training. Participants described activities–such as phishing simulation training, annual training, and awareness campaigns–that help employees understand cyber risks and how to behave securely. In their view, a human-centered approach ensured that awareness efforts were tailored, intuitive, and used different delivery modes. This concept also included clear, targeted communication of security information so that different groups of people can understand, listen, and act. Several interview participants emphasized that training is just one piece of a broader, holistic approach that also includes system design and security culture.

Human strengths. A few thought HCC included positively leveraging human abilities. These participants viewed people as integral, adaptive partners in security whose strengths are important to solving security problems.

3.2 RQ2: Who are the humans in HCC?

Interview participants overwhelmingly included a broad swath of people as the "humans" in HCC, going beyond the typical "general end users" to include anyone who touches or is impacted by an organization's cybersecurity program, such as security staff, leadership, developers, and customers. A few participants also included attackers as being within scope.

Survey participants were more divided. Across all survey participants, 95% indicated that General End Users are included, 66% Technical Professionals, 63% Decision Makers, 63% Communications and Learning Professionals, and 61% Policy and Regulatory professionals. Interestingly, less than half of General End Users believed that groups other than their own are included in HCC. In contrast, at least 70% of Human Factors/Behavior Specialists and more than half of the remaining groups thought that groups other than General End Users are included.

Disclaimer

Certain participant views are identified to foster understanding, not to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor to imply that these are necessarily the best available for the purpose.

Disclosure

The Introduction of this paper was edited with the assistance of Gemini (version 3), developed by Google. Gemini was used to refine language and condense content in accordance with the authors' instructions. All content, scientific claims, and conclusions have been reviewed and verified by the authors to ensure accuracy and originality.

Acknowledgments

This material is based upon work supported by University of Maryland, College Park NIST Professional Research Experience Program (PREP) under Award Number 70NANB23H024 and University of Maryland, Eastern Shore NIST PREP under Award Number 70NANB23H021.

References

[1] Gartner. Gartner identifies the top cybersecurity trends for 2023: Security leaders must pivot to a human-centric focus to establish an effective cybersecurity program. https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023, 2023.

[2] Marthie Grobler, Raj Gaire, and Surya Nepal. User, usage and usability: Redefining human centric cyber security. *Frontiers in Big Data*, 4:583723, 2021.

[3] Julie Haney, Matthew Canham, Mike Elkins, Lisa Flynn, Matthew Gordin, Victoria Granova, Wenjing Huang, Jody Jacobs, Greg Moody, Ann Rangarajan, Michael Ross, Robert Thomson, and Joe Uchill. NIST Special Publication 1332 - Workshop summary report for ConnectCon 2024: 'Minding the gaps in human-centered cybersecurity'. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1332.pdf, 2025.

[4] Julie M. Haney, Clyburn Cunningham, and Susanne Furman. Towards Bridging the Research-Practice Gap: Understanding Researcher-Practitioner Interactions and Challenges in Human-Centered Cybersecurity. In *19th Symposium on Usable Privacy and Security (SOUPS)*, 2024.

[5] Julie M. Haney, Clyburn Cunningham, and Susanne M. Furman. Towards Integrating Human-Centered Cybersecurity Research Into Practice: A Practitioner Survey. In *Symposium on Usable Security and Privacy (USEC)*, 2024.

[6] Keman Huang and Keri Pearlson. For what technology can't fix: Building a model of organizational cybersecurity culture. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, pages 6398–6407, 2019.

[7] Human-Centric Cybersecurity Partnership. Human-centric cybersecurity partnership. https://www.hc2p.ca/, 2026.

[8] Isto Huvila, Theresa Dirndorfer Anderson, Eva Hourihan Jansen, Pam McKenzie, and Adam Worrall. Boundary objects in information science. *Journal of the Association for Information Science and Technology*, 68(8):1807–1822, 2017.

[9] National Institute of Standards and Technology. Human-centered cybersecurity. https://csrc.nist.gov/projects/human-centered-cybersecurity, 2026.

[10] Networking and Information Technology Research and Development Subcommittee of the National Science and Technology Council. Federal cybersecurity research and development strategic plan. https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf, 2023.

[11] Jason RC Nurse, Joanna Milward, and Oz Alashe. From security awareness and training to human risk management in cybersecurity. In *International Conference on Human-Computer Interaction*, pages 86–104. Cham: Springer Nature Switzerland, 2025.

[12] Philip M. Podsakoff, Scott B. MacKenzie, and Nathan P. Podsakoff. Recommendations for creating better concept definitions in the organizational, behavioral, and social sciences. *Organizational Research Methods*, 19(2):159–203, 2016.

[13] Proofpoint. Human-centric security. https://www.proofpoint.com/us/threat-reference/human-centric-security, 2026.

[14] Robert Ramirez and Nazli Choucri. Improving interdisciplinary communication with standardized cyber security terminology: a literature review. *IEEE Access*, 4:2216–2243, 2016.

[15] Tufts University. Human-centered security and privacy. https://cybersecurity.tufts.edu/research/human-centered-security-and-privacy, 2026.

[16] Verena Zimmermann and Karen Renaud. Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies*, 131:169–187, 2019.

[17] Verena Zimmermann, Lorin Schöni, Thierry Schaltegger, Benjamin Ambuehl, Melanie Knieps, and Nico Ebert. Human-centered cybersecurity revisited: From enemies to partners. *Communications of the ACM*, 67(11):72–81, 2024.