AUTHOR VERSION

Advancing Human-Centered Cybersecurity: Challenges and Pathways Forward

Authors:

Anuradha Rangarajan, Illinois Institute of Technology
Julie Haney, National Institute of Standards and Technology
Matthew Canham, Cognitive Security Institute
Mike Elkins, Humanis Technologies
Lisa Flynn, University of Oulu
Matthew Gordin, RedPanda Systems
Victoria Granova, Amazon Web Services and Toronto Metropolitan University
Wenjing Huang, Alliance for Policy Research
Jody Jacobs, National Institute of Standards and Technology
Greg Moody, University of Nevada, Las Vegas
Michael Ross, Indiana University
Robert Thomson, Carnegie Mellon University
Joe Uchill, RAND Corporation

We present the key themes from the workshop "ConnectCon: Minding the Gaps in Human-Centered Cybersecurity," which can inform efforts of researchers and practitioners toward a collective goal of improving cybersecurity outcomes for all.

Introduction

Much of traditional cybersecurity focuses on technical defenses. Yet, there is increasing recognition that the sophistication of cyber threats directly targeting people and the well-documented role of the "human element" in cyber breaches [1] necessitate a different approach. Indeed, the critical factors of human behavior, limitations, motivations, cognitive biases, and decision making—as well as how organizational dynamics and culture reflect and influence those—are emerging as key to reducing vulnerabilities.

These factors are collectively bundled under the concept of "human-centered cybersecurity" (HCC). Although several complementary definitions for HCC exist, HCC is generally described as an approach and perspective that places people at the forefront when designing and implementing cybersecurity technologies and processes [2]; put simply, HCC is about making cybersecurity work for people and not the other way around. Ultimately, HCC aims to improve cybersecurity outcomes for organizations, individuals, and society by both reducing the likelihood of human error and leveraging human strengths.

Published in IEEE Security & Privacy, Volume 24, Issue 3, May-June 2026
https://www.computer.org/csdl/magazine/sp/2026/03/11519485/2gswsBXq8j6

Despite increasing awareness of the importance of the human element, many organizations fail to prioritize human-centered approaches to cyber defense. Barriers such as limited organizational awareness of human-centered impacts, lack of concrete guidance on how to take a human-centered approach, and the disconnect between academic research and real-world practice contribute to this challenge [3][4].

In both technical cybersecurity practitioner and research communities, there is a fundamental misunderstanding of human behavior and the interdisciplinary nature of cybersecurity. Measuring human-machine interactions and underlying motivations is often complicated by the perceived notion that human behavior is too complex to model [5]. Thus, defensive cybersecurity research has traditionally prioritized technical defenses over human experience, leading to technically robust, yet often unusable and inaccessible solutions. Coupled with the misconception that technical solutions create more "tangible" outputs and an attitude that trying to change human behavior is a futile endeavor, human-centric research investment has been traditionally under-prioritized.

Despite under-funding, a growing body of HCC research has emerged over the last two decades, with the human element recently being recognized as a research “cyber hard problem” critical for advancement of the cybersecurity field [6]. However, the transfer of that knowledge to practice is often hindered by siloed researcher and practitioner communities [3]. Divergent incentives among these communities (e.g. publishing and grant focus vs. profit-oriented product development) and the historical de-emphasis on HCC-related funding in organizations make collaborative progress difficult. This disconnect is exacerbated by research outputs that are behind paywalls and, at times, too abstract for practitioner consumption. Thus, organizations may fall behind in the latest HCC research developments, and researchers may struggle to keep up with practitioner needs.

It was against this backdrop, a field struggling with both a research-practice divide and a longstanding underinvestment in the human element, that the "ConnectCon: Minding the Gaps in Human-Centered Cybersecurity" workshop was convened. Held at the University of Nevada, Las Vegas, this opportunity created a forum to facilitate meaningful dialogue about the most pressing HCC challenges to organizations today. This unique event gathered 45 leading international experts from academia, government, and industry. With active presence in cybersecurity, participants' expertise spanned a variety of disciplines, including computer science, information technology, business operations, artificial intelligence, human factors, psychology, human cognition, and behavioral science. The workshop was organized by institutions having programs of special focus related to the human element in cybersecurity: Cognitive Security Institute, National Institute of Standards and Technology (NIST), Catalysts & Canaries Research Institute & Training Academy, and University of Nevada, Las Vegas.

During the workshop, keynote speaker and panel presentations served as catalysts for guided small group discussions that ultimately led to whole-group consensus on the top HCC challenges and strategies. The discussions leveraged the Holistic Operational Planning and Strategic Collective Implementation Planning (HOP/SCIP) methodology, a rapid ideation

Published in IEEE Security & Privacy, Volume 24, Issue 3, May-June 2026
https://www.computer.org/csdl/magazine/sp/2026/03/11519485/2gswsBXq8j6

technique created by Lisa Flynn, one of the workshop organizers. This technique, with roots in the Stanford Collective Impact model [7] serves to facilitate strategic planning and consensus-building across multidisciplinary teams.

In this article, we summarize the themes identified during the workshop[1]. For each theme, we describe the associated challenges as well as key questions—a non-exhaustive list derived from workshop attendee discussions—for addressing those challenges. These themes can inform researchers, practitioners, organizational decision makers, and guidance developers on forward-looking opportunities for collaboration, workforce development, and co-creative innovations for a resilient cyberspace.

Theme 1: A Shared Human-Centered Cybersecurity Agenda

The first theme identified during the workshop centers on the idea of a "shared agenda" for human-centered cybersecurity. This agenda includes, but is not limited to, standard language, goals, value propositions, guidelines, and associated measurements and organizational accountability structures within the HCC space.

Challenge: Lack of Common Ground

Workshop attendees identified the lack of common ground (mutual knowledge, beliefs, and assumptions) for HCC. The current landscape is cluttered with unclear language and divergent points of view on what constitutes HCC. For instance, the terms human factors, human risk management, usable security, and security awareness are often interchangeably used. Some view HCC as focused on mitigating human error and tempering "the weakest link", while others emphasize human strengths and aim to treat people as active partners in cybersecurity [8].

This challenge is compounded by the fact that, in a technology-dominated field, cybersecurity professionals and managers are not traditionally educated in HCC-related topics [4]. The knowledge gap—coupled with the current lack of authoritative guidance on how organizations can take a human-centered approach--can create uncertainty regarding when, how, and whether to implement and assess HCC interventions. The gap can also make it difficult for advocates of HCC to communicate a compelling value proposition to secure support from organizational leadership. Further, in the absence of clearly-defined HCC work roles, organizations may not recognize the competencies needed to effectively manage human-centered cybersecurity efforts in organizations.

A Clearer Conceptualization of Human-Centered Cybersecurity

[1] More details on the workshop program can be found in NIST Special Publication 1332 ***Workshop Summary Report for ConnectCon 2024: "Minding the Gaps in Human-Centered Cybersecurity"*** (https://doi.org/10.6028/NIST.SP.1332), upon which this article is based.

Addressing these symbiotic challenges requires the cybersecurity community to grapple with fundamental questions about how HCC should be defined, communicated, and operationalized:

- *What constitutes a shared HCC vocabulary?* While the need for common language is clear, how can diverse stakeholders, from academic researchers to practitioners to end users, collaboratively develop terminology that is both technically precise and practically meaningful? What elements should a standard description of HCC include to be useful across different organizational contexts? Can a single definition serve the field, or are context-specific adaptations necessary?
- *How can HCC demonstrate its value?* Beyond defining HCC, how should the field articulate its importance to organizational decision makers? What evidence or metrics would constitute a compelling value proposition? How can HCC be positioned not just as risk mitigation but as an enabler of broader organizational objectives?
- *What does codified HCC practice look like?* If the community were to develop recommended, outcome-based HCC practices, what form should these take to enable meaningful adoption by cybersecurity authorities, standards organizations, and research institutions? How can guidance be sufficiently specific to be actionable while remaining flexible enough for diverse organizational contexts? What role should case studies, training programs, and communication strategies play in socializing these practices?
- *Who is responsible for HCC in organizations?* As HCC matures, how should work roles and responsibilities be formalized? What competencies and skills are essential for professionals tasked with implementing human-centered approaches? How can organizations identify, develop, and recruit talent with the necessary interdisciplinary expertise? Where should HCC expertise sit within organizational structures: security teams, the human resources group, risk management, user experience, or elsewhere?
- *How does a shared agenda enable measurement and research?* A common framework could provide grounding for measuring HCC interventions (see Theme 2) and potentially address the innovation gap by making the value proposition more compelling. But what specific research questions become answerable with shared definitions and goals? How can standardization support rather than stifle innovation in this evolving field?

These questions represent critical areas where community consensus-building and collaborative research are needed to advance the field of human-centered cybersecurity.

Theme 2: Measuring Human-Centered Cybersecurity Impacts

A shared agenda for HCC enables organizations to develop their own tailored HCC outcomes: detailed, measurable statements that describe a desired result or change that happens because of actions taken. To determine the effectiveness of HCC interventions in achieving outcomes, organizations must measure impacts.

Published in IEEE Security & Privacy, Volume 24, Issue 3, May-June 2026
https://www.computer.org/csdl/magazine/sp/2026/03/11519485/2gswsBXq8j6

Challenge: Lack of Baselines to Measure Impact

Beyond the inherent difficulty of determining return on investment of cybersecurity in general, measuring HCC outcomes is particularly challenging. Without outcome-based measures of effectiveness, it can be hard to improve or adapt current efforts or justify continued investment in HCC efforts to organizational decision makers [4].

Organizations often lack an understanding of human factors or a baseline of past behaviors (both failures and positive actions), which complicates the development of meaningful human-centric metrics. In the absence of such baselines, organizations frequently turn to easy-to-capture but less meaningful measures as a proxy for real impact without putting concerted thought into what data and analysis are needed to truly make a determination of success. For example, current cybersecurity frameworks (e.g., the National Institute of Standards and Technology Cybersecurity Framework) do not currently include measurable HCC outcomes, mainly focusing on activity-based security awareness training metrics. Thus, organizations often emphasize the achievement of near-perfect training completion rates, diverting attention from the true desired outcome: evaluating whether the training drives sustained attitude and behavioral change.

Outcome-Driven Measurement Approaches

An outcome-based, iterative approach to measuring impact holds promise for providing organizations with the flexibility needed to achieve meaningful progress in HCC. However, critical questions remain about how to implement such an approach effectively:

- *Which HCC challenges should organizations prioritize within their specific contexts?* Recognizing that many organizations lack resources and deep expertise to address all HCC issues, how can organizations identify and select challenges that will make an immediate, positive difference? What methods can help surface both obvious friction points and hidden vulnerabilities?
- *How can organizations define meaningful HCC outcomes?* Many organizations are oriented towards meeting minimum compliance objectives (e.g., awareness training completion rates), rather than aspiring to outcomes that actually progress their organizations towards becoming more cyber resilient. What does "success" look like in the HCC space for different organizational contexts?
- *What types of interventions are most effective for achieving specific HCC outcomes?* How can organizations determine which approaches are worth investing in? Which interventions have HCC researchers evaluated, and how can those insights be tailored to individual organizations?
- *What metrics and measurement approaches can best capture the impact of HCC interventions on both individual behavior and organizational security posture?* While measures of effectiveness are often assumed to come in the form of quantitative metrics, how can organizations collect and utilize qualitative measures? How can

Published in IEEE Security & Privacy, Volume 24, Issue 3, May-June 2026
https://www.computer.org/csdl/magazine/sp/2026/03/11519485/2gswsBXq8j6

organizations build adaptive measurement strategies that allow them to learn from both successes and failures and adjust accordingly?
- *How can outcomes and measurements be best communicated?* How can the field articulate and demonstrate the direct contribution of HCC to technological and organizational outcomes in ways that resonate with decision makers?

To address these questions, closer collaboration is needed between measurement experts who can design rigorous instruments and practitioners who understand operational constraints. At a broader level, critical gaps remain in how cybersecurity frameworks and technical guidance incorporate HCC considerations and outcome-based measures.

Theme 3: Mental Load and Decision Making in Cybersecurity

Human decision-making is central to cybersecurity outcomes and is significantly influenced by psychological stressors and cognitive overload. Thus, an interdisciplinary approach is needed to better understand how workplace and personal stress and cognitive factors impact cyber resilience.

Challenge: Psychological Stressors and Cognitive Load

Psychological stressors can increase cognitive load, decrease self-efficacy, and impair decision making [9][10]. In the cyber world, these stressors and high cognitive load abound. The exponential growth of online information, the pressure to be "always-on," multitasking, and addiction to mobile devices contribute significantly to cognitive overload. As a result, individuals become more prone to making errors, particularly when tasks involve memory demands or are not perceived as relevant to the individual. Stressful personal or work circumstances amplify these negative outcomes, leading to lapses in judgment that increase susceptibility to cyber threats, especially attacks involving deception, such as phishing[11].

Cognitive overload also exacerbates security fatigue--the weariness and disengagement stemming from excessive or confusing security processes, technologies, and communications--and can be a driving factor behind ineffective responses to fear appeals (i.e., attempts to use fear to motivate better cyber hygiene). Ironically, cybersecurity professionals are especially vulnerable to cognitive overload due to untenable workloads and prolonged, high-pressure circumstances, which degrade decision-making and increase lapses in following standard operating procedures [12].

The evidence is clear: designing robust cybersecurity defenses must account for the complex interplay of human psychological and cognitive factors. Traditional cybersecurity frameworks often overlook these factors, leading to defenses that fail to adequately address the full spectrum of human behavior and decision-making.

Published in IEEE Security & Privacy, Volume 24, Issue 3, May-June 2026
https://www.computer.org/csdl/magazine/sp/2026/03/11519485/2gswsBXq8j6

Human-Centric Indicators of Cybersecurity Health

Workshop attendees suggested employee engagement platforms as a promising avenue for understanding the impact of psychological stressors and cognitive overload on cybersecurity behaviors and risk. However, significant questions remain about how such platforms should be designed and deployed:

- *What should be measured?* While potential metrics might include employee demographics, security behaviors (e.g., frequency of risky clicks or unauthorized access attempts), workplace factors (training, policies, attitudes), and psychological indicators [13], how can organizations determine which metrics are most predictive of cybersecurity risk in their specific contexts? What is the appropriate balance between breadth of data collection and focused, actionable insights?
- *How can psychological safety be measured and leveraged?* Research suggests that perceptions of psychological safety (the feeling that it is safe to speak up, make mistakes, and ask for help) may predict commitment to cybersecurity practices [14]. Yet critical questions remain: How can organizations accurately assess psychological safety without the measurement itself undermining trust? What organizational changes are most effective at promoting safety privilege—the assurance that employees won't face harm when reporting security concerns?
- *How can data collection protect employee privacy?* Any data collection raises fundamental ethical questions: What protections are necessary to ensure sensitive information is secured, used appropriately, and not leveraged for punitive purposes? How can organizations build employee trust in these systems? What role should employees play in determining what gets measured and how data is used?
- *What interventions do the data support?* Even with rich datasets, translating insights into action remains challenging: How can organizations move from correlation to causation when linking psychological stressors to specific vulnerabilities? What types of interventions—whether policy changes (flexible hours, mental health support), technological improvements (workflow simplification), or cultural shifts (recognition programs) —are most effective for different workforce segments? How can organizations validate that interventions actually reduce cognitive load and improve security behaviors rather than simply shifting the burden elsewhere?

Ultimately, the promise of human-centric measurement platforms depends on answering these questions through rigorous research and responsible experimentation in organizational settings.

Tailored Education and Learning Programs

Cybersecurity awareness training is often touted as the solution to positively aid in employee security decisions and behaviors. However, workshop attendees were concerned that generic, “one-and-done” training often falls short in adequately addressing the psychological stressors and overload employees often face. Instead, they advocated for organizations to engage in

continuous learning activities that are tailored to reflect and improve organizational security culture--"the beliefs, values, and attitudes that drive employee behaviors to protect and defend the organization from cyber attacks" [15]. Thus, the following salient questions warrant further reflection:

- *How can training promote a positive organizational security culture?* How can a people-centric cybersecurity learning culture be fostered so that employees are supported and encouraged to become active participants in cybersecurity? What strategies can help employees better understand how cybersecurity connects to their specific roles as well as the broader goals of the organization?
- *How can programs go beyond one-way, once-a-year training?* To reduce learning decay while minimizing training overload and fatigue, how often should learning be reinforced? What works in one organization or for one type of employee may not work in others; therefore, how can training programs be tailored to align with organizational culture and connect with employees who have varied learning styles, preferences on how they receive information, business functions, and stressors?
- *How can employees participate in informing and creating learning content and sharing responsibility for results?* What kind of feedback loops are most effective for ensuring content addresses the issues most relevant to employees and is meeting their needs?

A Call to Action

While some challenges, particularly those related to research funding priorities and the researcher-practitioner divide, require ecosystem-level change beyond any single organization, the following actions represent meaningful starting points for the broader cybersecurity and HCC communities.

As cybersecurity threats continue to evolve at an unprecedented rate, immediate and sustained collaboration between academia and industry is crucial to building a resilient workforce. Collective action is needed in several key areas including:

1. Building and continuing to foster cross-functional communities of experts that include fields such as psychology, behavioral economics, human-computer interaction, human factors, user experience design, and anthropology;
2. Establishing a shared understanding of the value proposition, terminology, and goals of HCC;
3. Accelerating the integration of HCC research into practice by focusing on cognitive security, behavioral interventions, and resilience-building strategies and incorporating actionable HCC guidance into technical standards and frameworks; and
4. Developing resources that support both practitioners and students in learning about and applying HCC principles.

Published in IEEE Security & Privacy, Volume 24, Issue 3, May-June 2026
https://www.computer.org/csdl/magazine/sp/2026/03/11519485/2gswsBXq8j6

ConnectCon 2024 marked an important first step toward achieving this vision and calls for ongoing action to establish human-centered cybersecurity as a central focus of cybersecurity strategy.

Disclaimer

Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Institute of Standards and Technology (NIST), the U.S. Government, or the authors' employers. Certain commercial companies or products are identified to foster understanding, not to imply recommendation or endorsement by NIST, nor to imply that these are necessarily the best available for the purpose.

References

[1] Verizon, “2025 Data Breach Investigation Report,” 2026, https://www.verizon.com/business/resources/reports/dbir/

[2] Networking and Information Technology Research and Development Subcommittee of the National Science and Technology Council, “Federal Cybersecurity Research and Development Strategic Plan,” 2023, https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf

[3] J. M. Haney, C. C. Cunningham, and S. M. Furman, "Towards bridging the research-practice gap: Understanding researcher-practitioner interactions and challenges in human-centered cybersecurity," in Proc. 19th Symp. Usable Privacy and Security (SOUPS), 2024.

[4] J. M. Haney, C. C. Cunningham, and S. M. Furman, "Towards integrating human-centered cybersecurity research into practice: A practitioner survey," in Proc. Symp. Usable Security and Privacy (USEC) at NDSS, 2024.

[5] R. Thomson and C. Lebiere, "Comparing similarity and homophily-based cognitive models of influence and conformity," in Proc. Int. Conf. Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation, pp. 47-57, Cham, Switzerland: Springer Nature, 2024.

[6] National Academies of Sciences, Engineering, and Medicine, “Cyber Hard Problems,” 2025, https://nap.nationalacademies.org/resource/29056/CyberHardProblems-2025.pdf

[7] J. Kania and M. Kramer. Collective Impact. Stanford Social Innovation Review, Winter 2011.

Published in IEEE Security & Privacy, Volume 24, Issue 3, May-June 2026
https://www.computer.org/csdl/magazine/sp/2026/03/11519485/2gswsBXq8j6

[8] V. Zimmermann, L. Schöni, T. Schaltegger, B. Ambuehl, M. Knieps, and N. Ebert, "Human-centered cybersecurity revisited: From enemies to partners," Commun. ACM, vol. 67, no. 11, pp. 72-81, 2024.

[9] Sterling, Peter. "Allostasis: a new paradigm to explain arousal pathology." Handbook of Life Stress, Cognition and Health (1988).

[10] Bandura, Albert. "Social foundations of thought and action." Englewood Cliffs, NJ 1986, no. 23-28 (1986): 2.

[11] Kim, Byung-Jik, Min-Jik Kim, and Julak Lee. "Examining the impact of work overload on cybersecurity behavior: Highlighting self-efficacy in the realm of artificial intelligence." Current Psychology 43, no. 19 (2024): 17146- 17162.

[12] Speelman, Craig, Craig Valli, and Oliver Guidetti. "Towards a method for examining the effects of cognitive load on the performance of cyber first responders." In Proceedings of the International Conference on Security and Management (SAM), pp. 41-47. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2019.

[13] W. Huang, S. Romanosky, and J. Uchill, "Beyond Technicalities: Assessing Cyber Risk by Incorporating Human Factors," Santa Monica, CA: RAND Corporation, 2025. https://www.rand.org/pubs/research_reports/RRA3841-1.html

[14] Lee, Daeun, Harjinder Singh Lallie, and Nadine Michaelides. "The impact of an employee's psychological contract breach on compliance with information security policies: intrinsic and extrinsic motivation." Cognition, Technology & Work 25, no. 2 (2023): 273-289.

[15] K. Huang and K. Pearlson, "For what technology can't fix: Building a model of organizational cybersecurity culture," in Proc. 52nd Hawaii International Conference on System Sciences, pp. 6398-6407, 2019.

Published in IEEE Security & Privacy, Volume 24, Issue 3, May-June 2026
https://www.computer.org/csdl/magazine/sp/2026/03/11519485/2gswsBXq8j6