

**NIST Special Publication (SP) 1332**

**Workshop Summary Report for  
ConnectCon 2024: “Minding the Gaps  
in Human-Centered Cybersecurity”**

Julie Haney  
Matthew Canham  
Mike Elkins  
Lisa Flynn  
Matthew Gordin  
Victoria Granova  
Wenjing Huang  
Jody Jacobs  
Greg Moody  
Ann Rangarajan  
Michael Ross  
Robert Thomson  
Joe Uchill

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.1332>

# NIST Special Publication (SP) 1332

## Workshop Summary Report for ConnectCon 2024: “Minding the Gaps in Human-Centered Cybersecurity”

Julie Haney  
*Information Technology Laboratory, NIST*

Matthew Canham  
*Cognitive Security Institute*

Mike Elkins  
*Vanguard*

Lisa Flynn  
*University of Oulu and Catalysts & Canaries  
Research Institute & Training Academy*

Matthew Gordin  
*Catalysts & Canaries Research Institute  
& Training Academy*

Victoria Granova  
*Amazon Web Services and Toronto  
Metropolitan University*

Wenjing Huang  
*RAND Corporation*

Jody Jacobs  
*Information Technology Laboratory, NIST*

Greg Moody  
*University of Nevada, Las Vegas*

Ann Rangarajan  
*Illinois Institute of Technology*

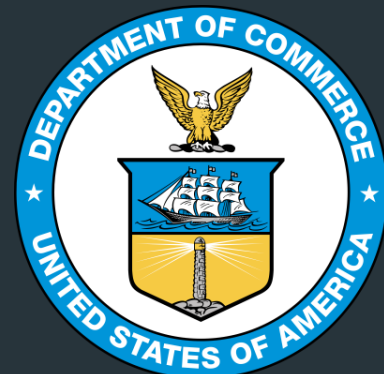
Michael Ross  
*Indiana University*

Robert Thomson  
*United States Military Academy*

Joe Uchill  
*RAND Corporation*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.1332>

APRIL 2025



U.S. Department of Commerce  
*Howard Lutnick, Secretary*

National Institute of Standards and Technology  
*Craig Burkhardt, Acting Under Secretary of Commerce for  
Standards and Technology and Acting NIST Director*

## Disclaimer

Certain commercial companies or products are identified in this report to foster understanding and provide details on the workshop. Further, this report summarizes the opinions of ConnectCon workshop attendees. These inclusions do not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that these are necessarily the best available for the purpose.

## NIST Technical Series Policies

[Copyright, Fair Use, and Licensing Statements](#)

[Technical Series Publication Identifier Syntax](#)

## Publication History

Approved by the NIST Editorial Review Board on: 2025-04-02

## How to cite this NIST Technical Series Publication

Haney, J. et al. (2025)

Workshop Summary Report for ConnectCon 2024: “Minding the Gaps in Human-Centered Cybersecurity”

National Institute of Standards and Technology

Gaithersburg, MD

NIST Special Publication (SP) 1332.

<https://doi.org/10.6028/NIST.SP.1332>

## NIST Author ORCID iDs

Julie Haney: 0000-0002-6017-9693

Jody Jacobs: 0000-0002-6433-884X

## Contact Information

[human-cybersec@nist.gov](mailto:human-cybersec@nist.gov)



## ABSTRACT

In August 2024, the National Institute of Standards and Technology (NIST) co-sponsored ConnectCon, an interactive workshop that facilitated meaningful conversations and connections between researchers and practitioners on the topic of human-centered cybersecurity. During the workshop, cybersecurity and human factors experts came to consensus on what they saw as the most pressing human-centered cybersecurity challenges today and potential solutions to address those challenges. This report provides an overview of the workshop as well as more detail about the identified challenges and solutions.

## KEYWORDS

cybersecurity; human-centered cybersecurity; human factors; workshop.



# TABLE OF CONTENTS

Introduction	<a href="#">1</a>
Workshop Overview	<a href="#">3</a>
Attendees and Organizers	<a href="#">4</a>
Program	<a href="#">5</a>
Challenges	<a href="#">9</a>
Challenge 1: The Innovation Gap	<a href="#">10</a>
Challenge 2: Lack of Shared Agenda for Human-Centered Cybersecurity	<a href="#">12</a>
Challenge 3: Measurement of Human-Centered Cybersecurity Impacts	<a href="#">13</a>
Challenge 4: Psychological Stressors	<a href="#">14</a>
Challenge 5: Cognitive Overload and Decision Fatigue	<a href="#">15</a>
Solutions	<a href="#">16</a>
Solution 1: Clearly Define Human-Centered Cybersecurity and Its Goals	<a href="#">17</a>
Solution 2: Develop Outcome-Based Guidance Focused on Measuring Impact	<a href="#">19</a>
Solution 3: Create Employee Engagement Platforms	<a href="#">20</a>
Solution 4: Build Tailored Education and Learning Programs	<a href="#">22</a>
Next Steps	<a href="#">24</a>
Beyond ConnectCon	<a href="#">25</a>
Acknowledgements	<a href="#">26</a>
References	<a href="#">27</a>

# INTRODUCTION

This report summarizes the program and outputs of ConnectCon, an August 2024 workshop co-sponsored by the National Institute of Standards and Technology (NIST) along with Cognitive Security Institute, Catalysts & Canaries Research Institute & Training Academy, University of Nevada Las Vegas, RedPanda Systems, and GuidePoint Security. The workshop brought together experts from industry, government, and academia to discuss the human element of cybersecurity.

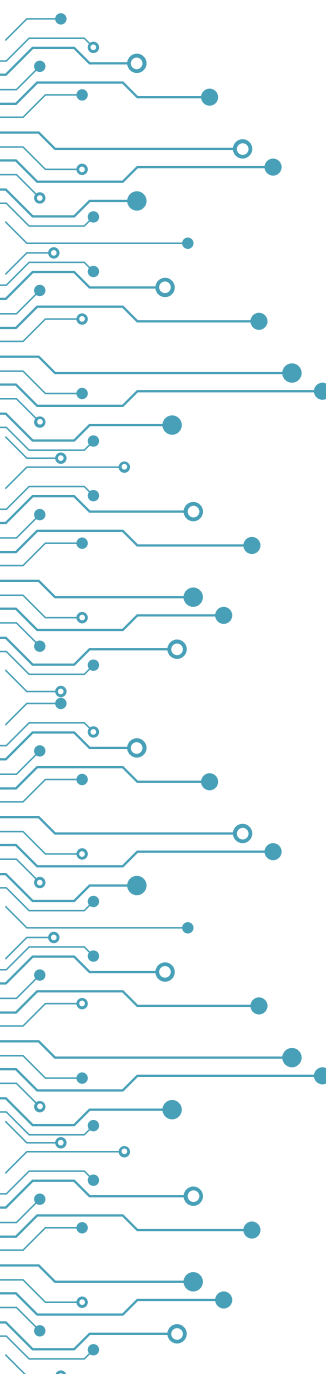
## Human-Centered Cybersecurity: Opportunities and Gaps

The cybersecurity community has traditionally relied upon technology to mitigate cyber risks. However, cyberattacks are increasingly exploiting people's roles, actions, unintentional errors, lack of knowledge, and the natural tendencies and predispositions that make us human [NSTC 2023][VERIZON 2024]. Thus, a greater emphasis on putting people at the forefront in cybersecurity is becoming widely recognized as critical to achieving positive cybersecurity outcomes for both individuals and organizations which, in turn, enable organizations to meet their business and mission objectives [GARTNER 2023a][NSTC 2023].

More broadly encompassed by the term *human-centered cybersecurity (HCC)*, this focus on people involves the relationships between the human, social, organizational, and technological factors in cybersecurity. For example, HCC includes factors related to people's cybersecurity needs, abilities, motivations, attitudes, perceptions, and behaviors. Without consideration of these factors, the stakeholders in cybersecurity (for example, end users, security professionals, organizational decision makers) may become increasingly frustrated, overwhelmed, uncertain, or disengaged while they and their organizations remain vulnerable to cyber threats [BUSSE 2019][NCA 2025][STANTON 2016].

As such, there are abundant needs and opportunities to:

- measure and manage human cyber risks and contributions
- create cybersecurity technologies and processes that work for people (not the other way around), and
- empower people to be active, capable partners in cybersecurity rather than being viewed as the "weakest link" [ZIMMERMANN 2024].



Despite the recognized importance of considering the human element, many organizations have yet to embrace a human-centered approach to cybersecurity. One stumbling block is the current lack of consensus on how organizations should go about recognizing and addressing HCC issues in practice. Further, researchers (who understand the science behind HCC) and practitioners (who have firsthand experiences of organizational practices) have been operating in out-of-sync silos [DHILLON 2021][HANEY 2024a][HANEY 2024b]. This disconnect can be detrimental to both communities, leaving little room to act upon and inform the others' efforts.

## ConnectCon 2024: Addressing the Gaps

ConnectCon 2024 aspired to address the gaps in HCC by creating a forum for meaningful, personal interactions in which researchers and practitioners could exchange ideas and make connections. Held in an interactive workshop format on August 9, 2024 at the University of Nevada, Las Vegas, ConnectCon brought together 45 thought leaders from industry, government, and academia. NIST's involvement in ConnectCon was a direct offshoot of recent NIST research on bridging the research-practice gap in HCC [HANEY 2024a][HANEY 2024b].

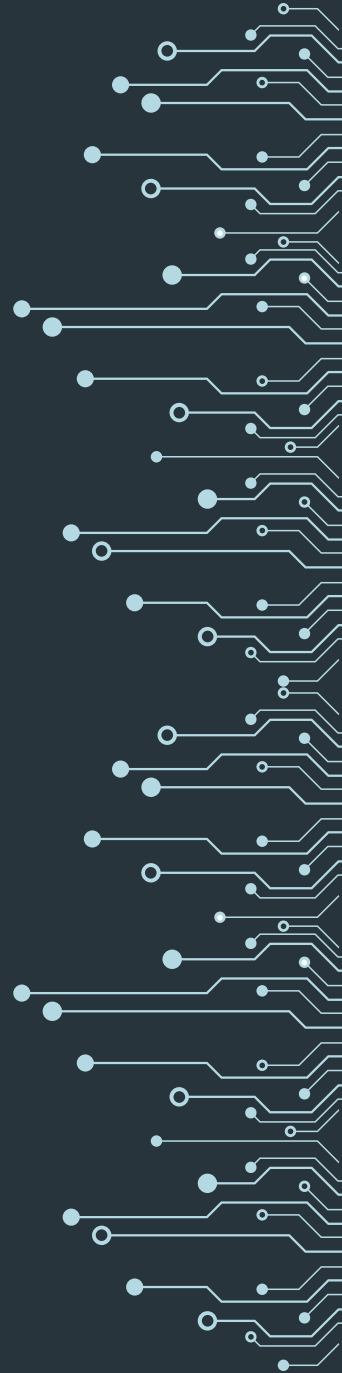
During the event, participants listened and learned about HCC issues and actively contributed to group discussions on HCC topics. The workshop aimed to identify current and emerging challenges related to the human element of cybersecurity as well as to explore pathways and solutions for collaboration, workforce development, and innovation to build a more secure and resilient world.

## About this Report

This report provides an overview of the workshop attendees, organizing committee, and program, followed by additional details to further expand upon each of the challenge and solution areas identified by ConnectCon participants.

The consensus-driven challenges and solutions can serve as a roadmap to inform and prioritize efforts of cybersecurity researchers, practitioners, decision makers, guidance developers, and vendors.

# WORKSHOP OVERVIEW





# ATTENDEES AND ORGANIZERS

In total, 45 individuals attended ConnectCon 2024, with 56% working in industry, 31% in academia, and 13% in national or state government (Fig. 1). All attendees were active in the cybersecurity field and invited specifically for their deep expertise in a variety of disciplines, such as computer science, information technology, business operations, artificial intelligence, human factors, psychology, human cognition, and behavioral science. Further, a number of participants were “boundary spanners” whose backgrounds straddled more than one sector or who had both research and practitioner experience.

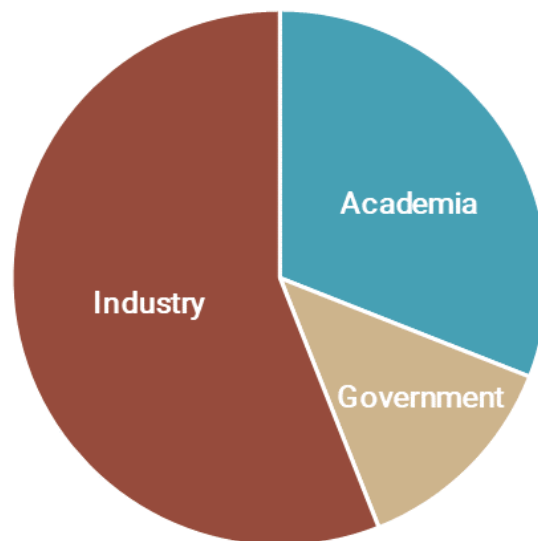


Figure 1. ConnectCon participants represented three types of organizations.

The ConnectCon organizing committee reflected the experiential breadth of workshop attendees and included:

- Matthew Canham, Cognitive Security Institute
- Lisa Flynn, University of Oulu and Catalysts & Canaries Research Institute and Training Academy
- Julie Haney, NIST
- Greg Moody, University of Nevada, Las Vegas

# PROGRAM

## Morning Session: Identifying Challenges

ConnectCon's morning session focused on identifying the "grand challenges" and needs in human-centered cybersecurity, with keynotes serving as thought-provoking catalysts for a subsequent roundtable discussion and rapid ideation exercise.

### Keynote Presentation

A joint keynote "debate" featured Perry Carpenter (Chief Human Risk Management Strategist, KnowBe4), who provided a practitioner perspective, and Dr. Arun Vishwanath (researcher and author in the field of cybersecurity, deception, and human behavior), who represented research. Lisa Flynn moderated the debate by delving into critical issues in human-centered cybersecurity, including the following overarching topics.

**Limits and constraints in cybersecurity:** recognizing the inherent limitations in cybersecurity frameworks, strategies, and prevailing attitudes, including:

- hesitance to share data and lack of data transparency
- desire for an "easy way out" by buying a packaged solution
- perception that humans are a lost cause
- doubt in the value of efforts to address the human element

**Semantics and nomenclature:** identifying the impact of inconsistent use and interpretation of terminology on communication and implementation, for example:

- misperception that "awareness training" implies that people will take the knowledge and act appropriately
- "human risk management" has both positive and negative connotations

**Monetization and funding:** exploring sustainable financial models and strategies for advancing human-centered cybersecurity research, such as:

- being able to tell a story with data
- communicating why research matters

**AI in the mix:** balancing the benefits and risks of incorporating AI in cybersecurity, for example:

- mitigating the weaponization of AI in cyber
- training people to recognize deep fakes
- opportunities for collecting and analyzing data to be more successful in cybersecurity

**"Sacred cows":** identifying outdated practices and concepts that need to be reevaluated or discarded, such as:

- the belief that "tech is the savior"
- trust in research that is neither methodologically rigorous nor transparent

## Facilitated Breakout Roundtables: Challenges

Following the keynote, Lisa Flynn led participants in facilitated, small-group breakouts to identify pressing challenges in HCC. Through structured brainstorming activities using the Holistic Operational Planning and Strategic Collective Implementation Planning (HOP/SCIP) rapid ideation methodology and a consensus-building voting session, the groups identified and elevated the following top challenges:

**Innovation gap:** the current environment in which adversaries are outpacing industry and research communities' capacities to keep up

**Lack of shared agenda for human-centered cybersecurity:** the absence of a standardized, common agenda for HCC

**Measurement of human-centered cybersecurity impacts:** uncertainty on how to measure the effectiveness of HCC efforts and interventions

**Psychological stressors:** psychological factors that contribute to or detract from individuals' capacity for cybersecurity behaviors

**Cognitive overload and decision fatigue:** external factors related to people's cybersecurity behaviors, attitudes, and risk

### RAPID IDEATION USING THE HOP/SCIP METHODOLOGY

The Holistic Operational Planning and Strategic Collective Implementation Planning (HOP/SCIP) methodology, developed by Lisa Flynn, is a structured approach designed to foster collaboration among participants with different backgrounds and areas of expertise. Rooted in Persuasive Systems Design [OINAS-KUKKONEN 2018], the HOP/SCIP methodology has ties to the Stanford Collective Impact model [KANIA 2011], aiming to break down silos while leveraging the unique insights of each participant to co-create solutions to complex problems. During the methodology, participants are guided through a series of fast-paced, interactive activities that encourage them to alternate between intuitive, rapid decision-making (System I thinking) and more deliberate, analytical reasoning (System II thinking). This cognitive shift allows participants to quickly identify and prioritize the most pressing issues while ensuring that solutions are not only innovative but also grounded in the collective expertise of the group. Through this dynamic process, the HOP/SCIP methodology enabled the ConnectCon participants to arrive at consensus-driven strategies that address key challenges in human-centered cybersecurity.

## Afternoon Session: Proposing Solutions

The afternoon session focused on possible solutions and ways to address the challenges in human-centered cybersecurity, both at a local or organizational level and more broadly. An expert panel shared their thoughts and insights to inspire a second roundtable discussion focused on solutions to the challenges identified in the morning session.

### Expert Panel

Julie Haney moderated the expert panel session featuring: Gabriel Bassett (Liberty Mutual Insurance), Rosanna Guadagno (University of Oulu), Calvin Nobles (University of Maryland Global Campus), and Robert Thomson (United States Military Academy). These panelists represented perspectives from industry, academia, and government.

The panel addressed the following key topics:

**Workforce education and training:** addressing the need for a multi-disciplinary approach and specialized training to address HCC

---

**Guidance and standards:** developing comprehensive frameworks, technical guidance, and standards that include HCC considerations

---

**Research collaboration:** encouraging stronger ties between academic research and practical implementation

---

**Tools and metrics:** identifying tools that effectively track and measure human-centric factors in cybersecurity

### Facilitated Breakout Roundtables: Solutions

In a continuation of the morning's discussions, Lisa Flynn facilitated the afternoon session in which participants reconvened in their groups to brainstorm actionable interventions and solutions for the identified challenges using the HOP/SCIP methodology. Solutions emerging from this consensus-building activity included:

---

**Clearly define human-centered cybersecurity and its goals:** Standardize terminology and HCC goals to provide a clear path and value proposition for organizations to implement HCC interventions.

---

**Develop outcome-based guidance focused on measuring impact:** Focus on measuring the effectiveness of HCC interventions, rather than compliance.

---

**Create employee engagement platforms:** Measure and track how psychological stressors, cognitive overload, and other predictors may be impacting cybersecurity within the organization.

---

**Build continuing education and learning programs tailored to organizational culture:** Ensure cybersecurity learning is relevant to individuals and customized to organizational culture.

---

### Ask/Give Session

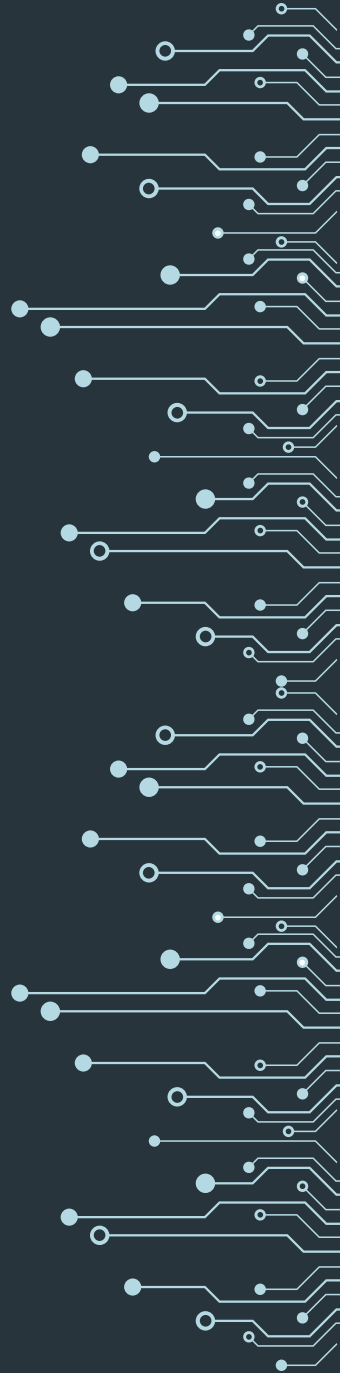
An "Ask/Give" session promoted partnerships and networking. During this session, participants were given an opportunity to speak to the full room and directly request and/or offer collaboration on future projects or research activities.

### Closing Remarks

Matthew Canham provided closing remarks on the criticality of considering the impact of "cognitive security" in our organizations and daily lives. The workshop ended with thanks to the participants, sponsors, and speakers, an emphasis on the importance of continued collaboration, and an invitation to participate in the [NIST Human-Centered Cybersecurity Community of Interest](#).

# CHALLENGES

In this section, ConnectCon participants expand upon the five most-pressing, interdependent human-centered cybersecurity challenges.



# CHALLENGE 1: THE INNOVATION GAP

Basic research into HCC has been limited by a reactionary funding environment that prioritizes short-term technical solutions over cognition-centric research. This mindset stifles innovation in its reliance on 40-year-old behavioral theories and the false notion that human decision-making is “too hard” to adequately capture at scale. Conversely, adversaries prioritize cognitive warfare and the information space because they are unable to compete in a kinetic fight with superior military forces.

ConnectCon participants identified the following four key issues that contribute to innovation gaps and underpin the other challenges identified during the workshop.

## Misunderstanding Human Behavior

Understanding how users interact with systems and what motivates their actions is complex and requires interdisciplinary research [DAWSON 2018]. It can be difficult to measure the effectiveness of human-centered approaches, and there may be a misunderstanding that human behavior is too complex to model effectively. These misunderstandings may stem from psychological theories that are 40+ years old and have not been well-validated to human cognition [THOMSON 2024]. Furthermore, traditional metrics of effectiveness may not capture user engagement and behavior changes adequately [ZIMMERMANN 2019].

## Siloed Researcher-Practitioner Communities

Researchers have different incentive structures compared with practitioners (e.g., publishing and grants-focused vs. product development and profit or mission-focused), and a lack of funding dollars in human-centered cybersecurity makes significant research progress challenging. Research that could best inform practice may also not be known by practitioners, difficult to find behind paywalls, and not in a form easily digestible and actionable for practitioners. Thus, it is challenging for researchers to keep up with practitioner needs, just as it is challenging for practitioners to keep up with evolving technologies and threats being identified by researchers [HANEY 2024a] [HANEY 2024b].

## Focus on Technical Solutions

Many cybersecurity solutions prioritize technical defenses (like firewalls, AI, and encryption) over user experience, often overlooking how humans engage with these systems [JEONG 2019]. This can lead to solutions that are secure but not user-friendly. Further, in many cases, the solutions do not generalize to the real-world from lab-based development. There is a misperception that technical solutions may be one-off while human-centered solutions are harder and require consistent interaction with human users. Therefore, funding tends to prioritize technical solutions (which have code snippets and products as a result) rather than human research (which may have less obviously measurable results).

## Adversary Flexibility

Many adversaries benefit from state support, providing them with significant resources for research and development in cybersecurity practices due to state prioritization of cyber operations over kinetic conflict. Adversarial nations may have fewer ethical guardrails regarding human research and human data, allowing them to support their own cyber operations and test their theories directly on civilian populations [SPITALETTA 2021].



## CHALLENGE 2: LACK OF SHARED AGENDA FOR HUMAN-CENTERED CYBERSECURITY

During the workshop, there was much discussion on the importance of HCC, with attendees acknowledging that considering the human element is critical for improved cybersecurity outcomes. However, as is often the case when a group of individuals with varied perspectives and backgrounds engage in discussion, workshop participants soon acknowledged that they—and other HCC researchers, cybersecurity practitioners, and organizational decision makers—may be lacking common ground (mutual knowledge, beliefs, and assumptions) about HCC.

In fact, the human element in cybersecurity is currently described using many different terms (e.g., human factors, human risk, usable cybersecurity, human-centered cybersecurity, human-centric security) and is often (mistakenly) conflated with security awareness training [CUNNINGHAM 2024]. Further, current views on HCC are often at odds; some primarily focus on human risk and failure, while others have a more positive view, seeing humans as partners and enablers in cybersecurity [ZIMMERMANN 2024].

Prior research suggests that barriers to organizations' consideration and integration of HCC principles may stem from a lack of awareness and knowledge of the concept as cybersecurity professionals and managers are not traditionally educated in this area [HANEY 2024a][NOBLES 2023]. This lack of knowledge leads to uncertainties about if, how, and when to implement and measure HCC interventions as well as difficulty communicating a strong HCC value proposition to gain support from organizational leadership.

At the core of these issues is the observation that the cybersecurity community has yet to standardize on a shared agenda for HCC. There are currently no standard HCC definitions, statements of importance/value proposition, enumeration of goals and associated measurements, nor common understanding of who is responsible for HCC within organizations.

## CHALLENGE 3: MEASUREMENT OF HUMAN-CENTERED CYBERSECURITY IMPACTS

Participants expressed that, in the cybersecurity field where it already can be difficult to measure return on investment, measurement of human behavioral aspects and their impact can especially be challenging [DEBRUIJN 2017] [DOYLE 2015]. This challenge is often due to a lack of understanding of human factors within the cybersecurity community, unreported cyber events that may victimize a large number of users, and the lack of “past mistakes” that can serve as baselines for human-centered measurements.

Workshop participants mentioned cybersecurity awareness training as a common example of the failure to measure impact. In many organizations, employees are required to complete annual training. The intent of this requirement is to facilitate positive, long-term impacts on workforce cybersecurity attitudes and behaviors, thus improving the overall security posture of organizations. However, despite these broader goals, organizations may focus on simple compliance with the mandate (i.e., training completion rates) and struggle to develop plans for or dedicate resources to determine whether their awareness programs actually positively impact behavior change [FERTIG 2020][JACOBS 2023].

This challenge symbiotically builds on *Challenge 2: Lack of a Shared Agenda for HCC*. The two combined have had a cascading impact on the ability of organizations to create and grow comprehensive HCC programs, for if cybersecurity professionals cannot point to concrete evidence showing the efficacy of HCC interventions, they cannot make a strong value proposition for HCC investment. An unintended, albeit critical consequence of this disinvestment is indifference among organizational employees and leaders, resulting in an “It’s not my problem” and “What’s in it for me” attitude about the human element. These attitudes may lead to a reactionary and defensive approach in responding to cyber events vs. a more proactive approach by predicting and preparing for them.

ConnectCon participants agreed that overcoming these barriers begins by articulating the benefits of HCC by answering the “right” set of questions:

- **What** is the value-proposition of adopting HCC practices to organizations?
- **How** can incorporating an HCC paradigm improve organizational risk posture?
- **Why** is it important to collect data on human security behaviors?
- **What** data should be collected?
- **Where** and **how** can organizations begin to collect and analyze such data?

Holistically reflecting on these seemingly simple questions can guide organizations in formulating corresponding solutions that measure and highlight the effectiveness of HCC investments beyond the mere act of tracking human “activities” in a cybersecurity context.

## CHALLENGE 4: PSYCHOLOGICAL STRESSORS

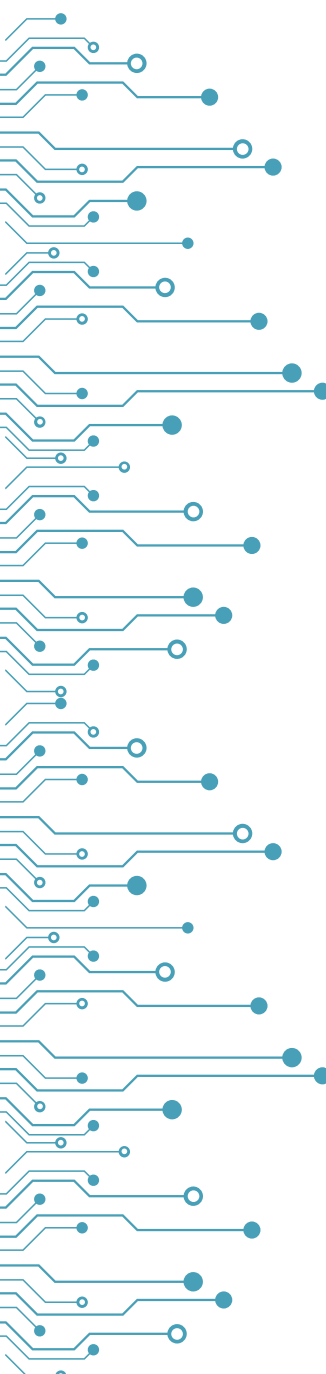
Cybersecurity professionals have long recognized the human factor as a persistent vulnerability in digital security [NOBLES 2022] [SCHNEIER 2015]. However, traditional cybersecurity frameworks often fail to account for the psychological stressors that shape individuals' online behaviors. Integrating insights from psychoneuroimmunology, social cognitive theory, and trauma research provides a more holistic perspective on why users engage in risky digital behaviors and how chronic stress may compromise cyber resilience.

Psychoneuroimmunology explores how stress influences immune function and cognition [ADER 1995]. Chronic exposure to psychological stressors—whether from workplace demands, financial insecurity, or personal trauma—can lead to dysregulated cortisol levels and cognitive impairment [MCEWEN 1993]. This phenomenon, conceptualized as cognitive allostatic load, affects decision-making and impulse control, increasing susceptibility to deception-based cyber threats like phishing and other social engineering attacks [STERLING 1988]. Adverse experiences and cognitive allostatic load can increase inflammation from stress and increase vulnerability to mental health struggles such as depression and anxiety, which may impact decision-making and motivation [SLAVICH 2014][MCCLOUGHLIN 2014].

Social cognitive theory provides further context for understanding human vulnerability in cyberspace. Agency (ability to make one's own decisions), self-efficacy (one's belief in their ability to complete a task or achieve a goal), and reciprocal determinism (idea that behaviors are controlled by the individual) all play a role in shaping behavior [BANDURA 1986]. Under conditions of high stress, individuals experience diminished self-efficacy and distress tolerance, which may lead to poor digital behaviors, such as weak password management or disengagement from cybersecurity protocols [BANDURA 2001]. This is potentially exacerbated by online disinhibition, which is the tendency to behave differently online due to factors like anonymity and psychological distancing [SULER 2004]. Online disinhibition has been associated with depression and emotional regulation challenges [SYRJAMAKI 2024][ANTONIADOU 2019]. Cybercriminals will exploit these cognitive vulnerabilities, manipulating users through deception, coercion, and AI-enhanced techniques.

Ultimately, the integration of psychological stressors from a psychoneuroimmunological perspective, with the disinhibition model [SULER 2004] and agentic framework [BANDURA 1986] serving as contextualizing forces, may provide a more comprehensive understanding of cybersecurity's human factor. Cyber resilience strategies should – but often do not – incorporate behavioral health and trauma-responsive models, acknowledging the impact of stress on agency in shaping digital risk behaviors [BANDURA 1982][KARADEMAS 2003]. As cybersecurity threats become increasingly sophisticated, an interdisciplinary approach that includes behavioral science is essential for mitigating human vulnerabilities in the digital landscape.

## CHALLENGE 5: COGNITIVE OVERLOAD AND DECISION FATIGUE



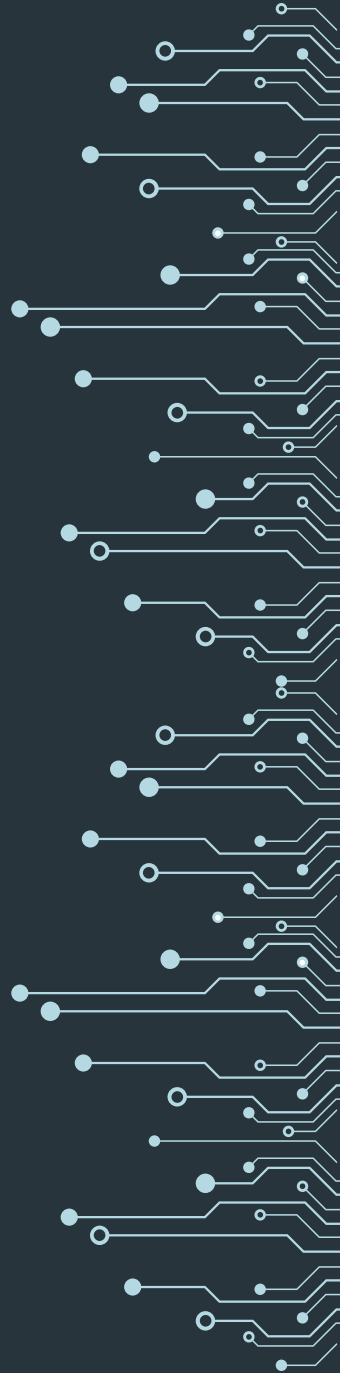
Cognitive overload is one of the contributing factors to the wave of burnout and fatigue that is the result of an always-on work mentality coupled with an increasing amount of socializing coming from online sources (e.g., social media, gaming). The sheer volume of online information, number of incoming emails, and addiction to mobile devices has led to many people feeling physically and emotionally overwhelmed [RAYWOOD-BURKE 2023][SHENG 2023][GANYE 2024]. In general, when performing tasks that require high memory demands, especially under stressful conditions (as described in *Challenge 3: Psychological Stressors*), performance decreases and errors are more likely to occur. Cognitive overload may occur in either tasks with sufficiently high working memory load, those requiring divided attention, and/or those requiring multi-tasking.

While a societal issue affecting many aspects of modern life, the consequences of overload substantially and negatively impact (cyber)security behaviors. In practice, strains on working memory [HINSON 2003] can lead to impulsive-type behaviors. Impulsiveness has routinely correlated with a variety of bad security behaviors [HADLINGTON 2017][AIVAZPOUR 2019][MODIC 2012]. For instance, high cognitive load appears to limit the necessary attention to detail needed to deflect phishing emails [WANG 2012], and cognitive load appears to be a factor in the effectiveness of appealing to fear to improve employee cyber hygiene practices [GAYNE 2024][BERNARD 2021]. Further, there are an array of cognitive factors in security-specific burnout (“security fatigue”) that impact employees overloaded with security messaging and training [REEVES 2021].

Cognitive overload is not just limited to those without specialized cybersecurity expertise. Rather, overload can and often impacts cybersecurity professionals. Current workloads in cybersecurity roles are unsustainable, with often-rote, attentionally-demanding tasks conducted under time-pressure and with substantial uncertainty over the quality and availability of information [ALESCÉ 2023][CHOWDURY 2019][HULL 2017]KIM 2024][SPEELMAN 2024]. Furthermore, the societal reliance on technology, lack of work-life balance, and other extrinsic factors described above have limited current cybersecurity professionals from recovering from their work [NOBLES 2022]. These pressures have been directly associated with reduced work performance and negative security outcomes due to impaired decision-making and increases in workplace errors, including ignoring rules and standard operating procedures [ALECSE 2023][YENG 2022].

# SOLUTIONS

ConnectCon participants prioritized potential solutions to the human-centered cybersecurity challenges identified in the morning session. These solutions are often interdependent and may address more than one challenge.



# SOLUTION 1: CLEARLY DEFINE HUMAN-CENTERED CYBERSECURITY AND ITS GOALS

In response to *Challenge 1: The Innovation Gap* (specifically, the misunderstanding of human behavior) and *Challenge 2: Lack of Shared Agenda for HCC*, ConnectCon participants recommended standardizing on a clear description of HCC in order to develop a shared language that can be used and understood by different stakeholders.

Participants suggested that this common description be developed using a rigorous, systematic process that builds consensus across different stakeholder groups in cybersecurity (e.g., academic researchers, practitioners, decision makers, human factors experts, end users).

Attendees also emphasized that, while the establishment of a standard description is foundational, ultimately, this description could be further tailored to the specific human strengths, needs, and risks of individual sectors and organizations.

## Describing Elements of Human-Centered Cybersecurity

The standard description of HCC could include:

a **definition** to succinctly communicate what HCC is

a **statement of importance** to convey the benefits of taking a human-centered approach, not just in terms of managing human risk but also how human strengths could contribute to cybersecurity

**dimensions** of HCC to provide clarity on aspects of cybersecurity with the potential to positively or negatively influence people's cybersecurity engagement and behaviors

**measurable goals** to communicate what human-centered cybersecurity hopes to achieve—for example, the desired end state with respect to organizational cybersecurity or an objective for how employees play a role in cybersecurity

## Leveraging the Standard

Once developed, the HCC definition and goals could then be used as a foundation to:

**Codify and recommend HCC practices** for organizations.

---

**Measure** whether HCC interventions have made an impact.

---

**Develop training and other communications** to educate the cybersecurity community and organizations on HCC, including human risks and strengths and how to manage those.

---

**Share HCC case studies** that demonstrate success or lessons learned.

---

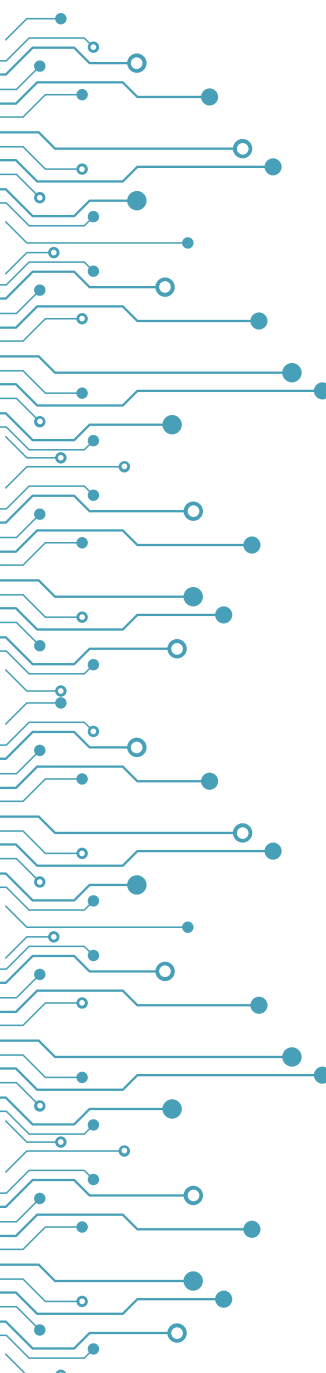
**Understand HCC roles and responsibilities** within organizations.

---

**Recruit professionals** with the skills necessary to integrate HCC into organizational practices.

---

**Encourage collaboration** between HCC researchers and practitioners.



## SOLUTION 2: DEVELOP OUTCOME-BASED GUIDANCE FOCUSED ON MEASURING IMPACT

Addressing *Challenge 3: Measurement of HCC Impacts*, ConnectCon participants discussed the need for organizations to shift away from simply tracking human activities and compliance metrics (e.g., percentage of employees completing awareness training or click rates for simulated phishing exercises) towards instead measuring the impact and demonstrating the value of HCC interventions.

This shift is predicated on an iterative, outcome-based approach to HCC in which organizations:

**Identify HCC issues:** Determine and prioritize current HCC challenges in the organization.

**Define HCC outcomes:** Determine the desired changes or end state.

**Develop interventions and activities:** Create solutions to help achieve the outcomes.

**Measure HCC outcomes:** Collect data and track progress to see if the outcomes are being achieved.

**Adjust plans:** Use the measurement results to improve plans for achieving the outcomes.

This approach specifies a desired end state, leaving the details of how to achieve that end state up to individual organizations [FUKUDA 2019]. While this non-prescriptive approach can allow for greater flexibility and foster innovation, organizations may be at a loss as to what and how to measure to determine whether outcomes have been achieved [JACOBS 2023]. Therefore, there will be a need to bring in human measurement experts to determine meaningful measures, develop measurement instruments, and validate those within operational settings. Solution 3 delves deeper into examples of the types of measurements that might be helpful for determining whether outcomes have been met and identifying potential human risks needing to be addressed in the first place.

ConnectCon participants viewed *Solution 1: Clearly Define HCC and Its Goals* as a foundational step to help establish criteria against which specific outcomes can be established. They also recommended that more industry and government cybersecurity frameworks and technical guidance incorporate HCC considerations and outcomes (few currently do) and clearly communicate how HCC is integral to technology outcomes (e.g., user acceptance or correct use).



## SOLUTION 3: CREATE EMPLOYEE ENGAGEMENT PLATFORMS

ConnectCon participants proposed that vendors and researchers develop employee engagement platforms, which could address *Challenge 4: Psychological Stressors*, *Challenge 5: Cognitive Overload and Decision Fatigue*, and, in part, *Challenge 1: The Innovation Gap*. Grounded in psychology, behavioral science, cognitive science, and human factors, an engagement platform focuses on identifying employee cybersecurity issues that need to be addressed, predicting potential human risks, and tracking progress within the organization to mitigate those risks. Additionally, the platform can provide a means through which to promote a strong cybersecurity culture within the organization by engaging employees in a variety of interactive and informative ways that build awareness, motivate, and empower them to take an active role in cybersecurity.

### Collecting Metrics

To identify risks and track progress in addressing those, the platform would collect employee and organizational cybersecurity health metrics that are predictive of cybersecurity behaviors and risks. These HCC measurements exist both as an array of behavioral, non-security predictors and as a measurement of actual security behavior. The latter can be particularly telling: organizations can compile individual propensities to act securely (e.g. their frequency of clicking on things they should not click, or attempts to access things they should not access). However, measurements based on past mistakes require past mistakes. Thus, non-security predictors can give practitioners the opportunity to attempt to mitigate that first mistake as well as subsequent mistakes. These predictors might include: individual factors (e.g., demographics, personality traits, life circumstances, or knowledge, skills, and abilities); workplace factors (e.g., cognitive load, training, organizational policy, attitudes about the organization); or external threats (e.g., how hackers value and target people) [HUANG 2024].

Attendees provided examples of metrics that platforms might collect. Platforms could assess the cybersecurity impact of psychological stressors and cognitive overload (e.g., antecedents to burnout) via validated psychometric tools from the fields of clinical psychology and social work that may be adapted to assess digital vulnerabilities. For example, the Depression Anxiety Stress Scale-21 (DASS-21) is a widely used instrument for measuring psychological distress and cognitive load [LOVIBOND 1995][MOYA 2022]. It is possible that by incorporating DASS-21 assessments into cybersecurity research and workforce engagement platforms – with the appropriate protections for this sensitive information – professionals can better understand how chronic stress impairs cyber decision-making and develop more targeted interventions [PAPPA 2024]. Further, measurements of employee perceptions of psychological safety and perceived breaches of the psychological contract with their organizations may predict their commitment

to cybersecurity within the organization [KATCHER 2024][LEE 2023]. Metrics on psychological stressors and overload could also be compared to common hacker techniques to identify potential areas of human vulnerability.

## Informing Solutions and Mitigations

Metrics collected by an engagement platform could then be used to inform HCC solutions and risk mitigations that resonate with employees and prompt organizational commitment, trust, and positive cybersecurity behaviors in the long term.

ConnectCon attendees offered several examples of how metrics could drive solutions:

**Training updates** could reflect newly identified risks to the organization.

---

Identification of psychological stressors related to organizational changes could lead to an **adjustment of messaging** around change initiatives.

---

Metrics indicating negative feelings of psychological safety could inform efforts to instill a sense of “**safety privilege**” within the organization so that employees can feel comfortable bringing attention to security issues without fear of reprisal.

---

Indicators of high cognitive load might be addressed by implementing **extrinsic incentives** to limit stress (e.g., sufficient salary, time off, flexible work hours) as well as **intrinsic incentives** (e.g., mental health support, optimal training).

---

Indicators of employee successes and positive behaviors could inform **reward or recognition efforts**.

---

**Technology and process improvements** could address identified decision-fatigue by limiting some of the more menial tasks (e.g., threat alert triage), optimizing software interfaces, and increasing usability.

## SOLUTION 4: BUILD TAILORED EDUCATION AND LEARNING PROGRAMS

ConnectCon participants proposed another solution to *Challenge 4: Psychological Stressors* and *Challenge 5: Cognitive Overload and Decision Fatigue*: building continuing education and learning programs that are tailored to organizational culture. This proposal can have a bidirectional relationship with *Solution 3 Create Employee Engagement Platforms* as it can be informed by metrics collected in the platform while also informing adjustments to platform metrics and training resources.

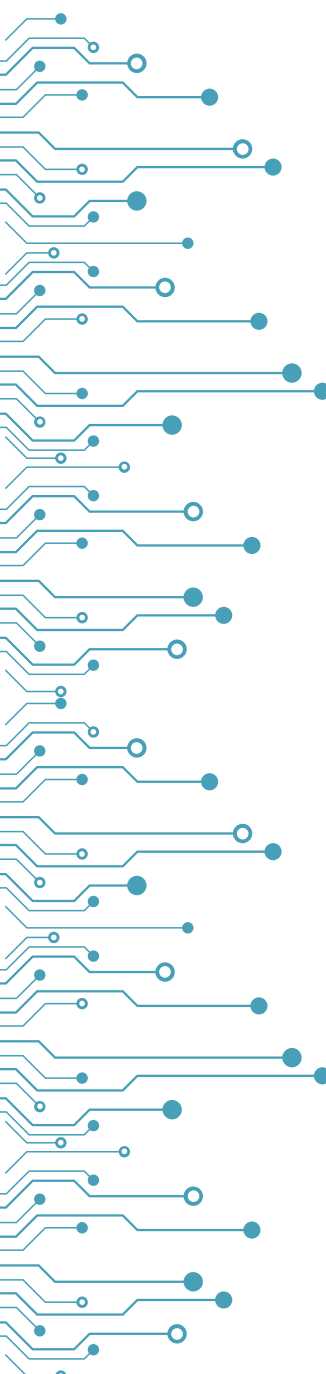
### Promoting Continuous Learning

Participants stressed the importance of continuous learning rather than less-effective, once-a-year training that often fails to positively change employee cybersecurity attitudes and behaviors in the long term [ALSHAIKH 2021][BADA 2019]. Participants believed that successful cybersecurity awareness and training programs are those that reinforce learning throughout the year by using a variety of engaging methods that appeal to the different learning styles and preferences of employees, for example, via micro-learning, cybersecurity ambassadors/champions programs, gamification, and in-person and interactive activities.

### Tailoring to Organizational Culture

Importantly, participants emphasized that learning should be tailored to and in support of strengthening the organizational cybersecurity culture and protection from organization-specific cyber risks with a focus on the “people” aspect of the People, Process, Technology information technology framework [GARTNER 2023b]. Organizational culture can be defined as the values, assumptions, and artifacts held by its workforce [SCHEIN 2010]. Similarly, cybersecurity culture encompasses the values, beliefs and behaviors around interacting with and protecting an organization’s information assets [DAVEIGA 2010][FLORES 2016]. The extent to which employees align to the organizational culture and demonstrate the culture can significantly increase employee performance – by up to 22% [GARTNER 2024]. It follows that encouraging training alignment with an organizational cybersecurity culture would improve cybersecurity performance.

Thus, to contextualize education and learning, ConnectCon attendees recommended communicating the relevance of cybersecurity to the organization and specific work roles, as employees need a reason to care about cybersecurity [DEBRUIJN 2017]. First, employees at all levels must see the business value of cybersecurity within the organization – for example, how cybersecurity enables the mission, who and what it protects, and how it ensures revenue and protects reputation. Then, beyond organizational relevance, participants suggested that education be tailored to different work roles so that employees recognize their own personal responsibility for



cybersecurity and become intrinsically motivated to practice strong cybersecurity habits. Yet participants expressed that simple awareness is not enough; education and learning efforts also need to empower employees by providing actionable guidance that can be taken given their roles, knowledge, skills, abilities, and the psychological and cognitive stressors they typically encounter at work.

### **Encouraging Employee Participation**

Participants further emphasized that employee participation in formulating a learning program is key. Attendees recommended that programs solicit and act upon employee feedback and needs, continually measure the effectiveness of training on employee attitudes and behaviors, and use feedback to adjust course as necessary. In addition to quantitative metrics, programs can gather qualitative data directly from employees, for example, via surveys or focus groups.

# NEXT STEPS



# BEYOND CONNECTCON

ConnectCon successfully brought together multiple stakeholders in human-centered cybersecurity, identifying key challenges and generating actionable solutions. The event highlighted the need for ongoing collaboration, innovative research, and integrated practices to address the evolving landscape of cybersecurity threats. While participants left with a shared vision for building a more resilient cybersecurity workforce and ecosystem, they agreed that there is more to be done to keep momentum going. In particular, the following strategic areas and questions would be helpful in moving the cybersecurity community forward.

**Building community:** How can we grow and nurture supportive, multidisciplinary groups (e.g., NIST HCC Community of Interest and Cognitive Security Institute) that value information sharing and work towards closing the gap between the science/research of HCC and practice? How can we foster collaboration between cybersecurity professionals and experts in other fields (such as psychology, behavioral economics, UX design, and anthropology) to strengthen cybersecurity strategies? How can these groups be leveraged to tackle hard problems in HCC? Who should take the lead on building these communities?

**Consensus on human-centered cybersecurity:** What are the shared terminologies, goals, and measurements of HCC? What is the value proposition of HCC? How can the community be leveraged to build consensus? How can we better communicate the business case for HCC to CISOs, board members, and policymakers to ensure organizational commitment?

**Translating research into application:** How can we accelerate the application of human-centered cybersecurity research into real-world cybersecurity strategies? What mechanisms can be put in place to ensure continuous dialogue between researchers and practitioners? How can HCC inform a more holistic approach to managing human risk beyond training by incorporating cognitive security, behavioral interventions, and resilience-building?

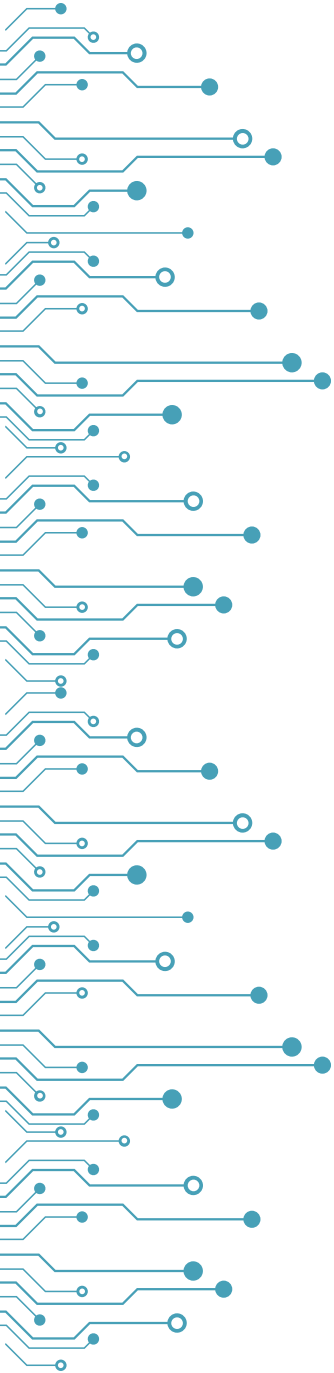
**Integration of actionable HCC considerations into technical guidance and standards:** How can we incorporate HCC directly into technical guidance, standards, and other practitioner-focused resources so that HCC is seen as an integral part of any cybersecurity strategy and implementation and not an afterthought? How do we develop metrics and key performance indicators (KPIs) that clearly demonstrate the effectiveness of human-centered approaches in cybersecurity risk reduction? How can these be communicated to executives and stakeholders?

**Developing a training program:** How do we develop resources and training (e.g., professional certifications, conference tracks, formal education curricula) for practitioners so they can learn about HCC, how to integrate it into practice, and how to obtain buy-in within their organizations? How can we create and sustain open-access repositories for HCC tools, frameworks, case studies, and best practices?

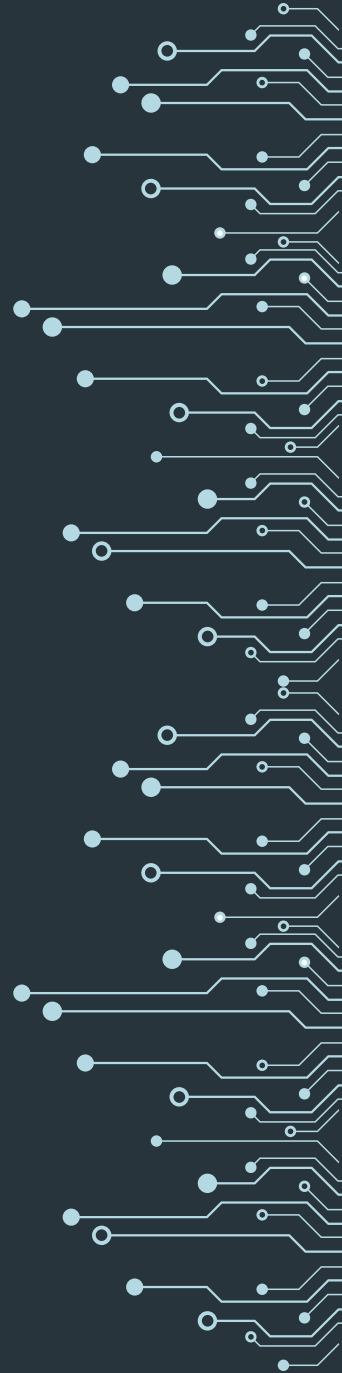
---

# ACKNOWLEDGEMENTS

Thanks to the ConnectCon attendees and co-sponsors for their valuable participation and contributions. Special thanks to the student coordinators who assisted with workshop logistics and the rapid ideation activities: Francis Hahn from University of South Florida, and Matthew Gordin, Eliel Ehimare, and Pardis Shabaani from Catalysts & Canaries Research Institute & Training Academy.

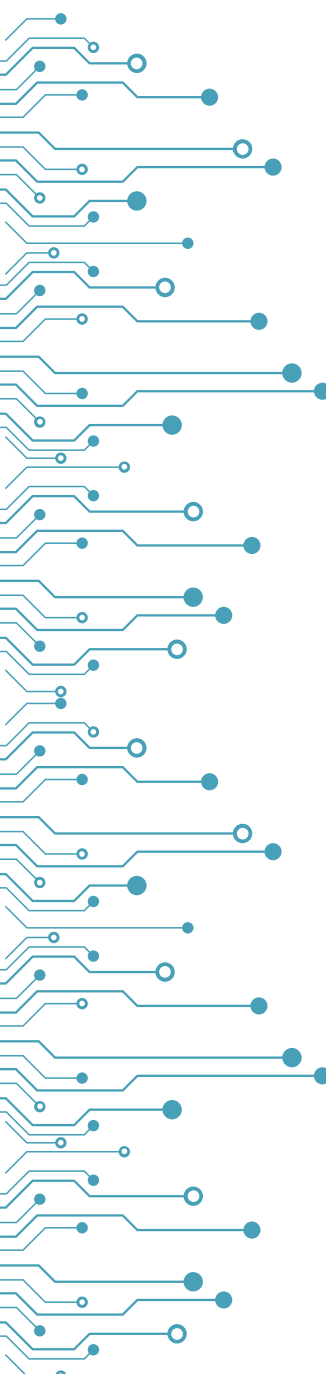


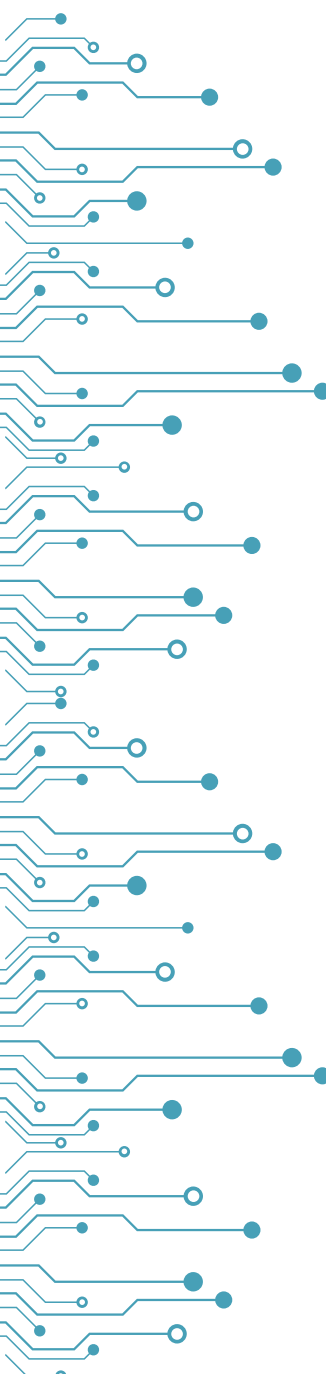
# REFERENCES





## REFERENCES

- 
- [ADER 1995] Ader, Robert, and Nicolas Cohen. "Psychoneuroimmunology: interactions between the nervous system and the immune system." *The Lancet* 345, no. 8942 (1995): 99-103.
- [AIVAZPOUR 2019] Aivazpour, Zahra, and V. Srinivasan Rao. "Impulsivity and information disclosure: implications for privacy paradox." (2019).
- [ALECSE 2023] Alecse, Cristian. "The Impact of Choice Overload on Decision Deferral in Cybersecurity." *The Journal of the Southern Association for Information Systems* 10, no. 2 (2023): 1-11.
- [ALSHAIKH 2021] Alshaiikh, Moneer, and Blair Adamson. "From awareness to influence: toward a model for improving employees' security behaviour." *Personal and Ubiquitous Computing* 25, no. 5 (2021): 829-841.
- [ANTONIADOU 2019] Antoniadou, Nafsika, Constantinos M. Kokkinos, and Angelos Markos. "Psychopathic traits and social anxiety in cyber-space: A context-dependent theoretical framework explaining online disinhibition." *Computers in Human Behavior* 99 (2019): 228-234.
- [BADA 2019] Bada, Maria, Angela M. Sasse, and Jason RC Nurse. "Cyber security awareness campaigns: Why do they fail to change behaviour?." *arXiv preprint arXiv:1901.02672* (2019).
- [BANDURA 1982] Bandura, Albert. "Self-efficacy mechanism in human agency." *American Psychologist* 37, no. 2 (1982): 122.
- [BANDURA 1986] Bandura, Albert. "Social foundations of thought and action." *Englewood Cliffs, NJ* 1986, no. 23-28 (1986): 2.
- [BANDURA 2001] Bandura, Albert. "Social cognitive theory: An agentic perspective." *Annual Review of Psychology* 52, no. 1 (2001): 1-26.
- [BERNARD 2021] Bernard, Leon, Sagar Raina, Blair Taylor, and Siddharth Kaza. "Minimizing cognitive overload in cybersecurity learning materials: an experimental study using eye-tracking." In *IFIP World Conference on Information Security Education*, pp. 47-63. Cham: Springer International Publishing, 2021.
- [BUSSE 2019] Busse, Karoline, Julia Schäfer, and Matthew Smith. "Replication: No one can hack my mind revisiting a study on expert and {Non-Expert} security practices and advice." In *15th Symposium on Usable Privacy and Security (SOUPS 2019)*, pp. 117-136. 2019.

- 
- [CHOWDHURY 2019] Chowdhury, Noman H., Marc TP Adam, and Geoffrey Skinner. "The impact of time pressure on cybersecurity behaviour: a systematic literature review." *Behaviour & Information Technology* 38, no. 12 (2019): 1290-1308.
- [CUNNINGHAM 2024] Cunningham, Margaret, Calvin Nobles, Nikki Robinson, and Julie Haney. "Leveraging the Human Factors Discipline for Better Cybersecurity Outcomes: A Roundtable Discussion." *IEEE Security & Privacy* 22, no. 6 (2024): 99-104.
- [DAVEIGA 2010] Da Veiga, Adéle, and Jan HP Eloff. "A framework and assessment instrument for information security culture." *Computers & Security* 29, no. 2 (2010): 196-207.
- [DAWSON 2018] Dawson, Jessica, and Robert Thomson. "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance." *Frontiers in Psychology* 9 (2018): 744.
- [DEBRUIJN 2017] De Bruijn, Hans, and Marijn Janssen. "Building cybersecurity awareness: The need for evidence-based framing strategies." *Government Information Quarterly* 34, no. 1 (2017): 1-7.
- [DHILLON 2021] Dhillon, Gurpreet, Kane Smith, and Indika Dissanayaka. "Information systems security research agenda: Exploring the gap between research and practice." *The Journal of Strategic Information Systems* 30, no. 4 (2021): 101693.
- [DOYLE 2015] Doyle, Kenny, Zeta Dooly, and Paul Kearney. "What's so unique about cyber security?." In *Cyber Security and Privacy Forum*, pp. 131-139. Cham: Springer International Publishing, 2015.
- [FERTIG 2020] Fertig, Tobias, Andreas Erwin Schütz, and Kristin Weber. "Current Issues Of Metrics For Information Security Awareness." In *European Conference on Information Systems*, vol. 11, pp. 19-20. 2020.
- [FLORES 2016] Flores, Waldo Rocha, and Mathias Ekstedt. "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness." *Computers & Security* 59 (2016): 26-44.
- [FUKUDA 2019] Fukuda, Yuki, Isamu Kawamura, Yoshihiro Kubota, and Yoshiro Wataguchi. "Supply chain security measures using outcome-based approach." *Fujitsu Scientific & Technical Journal* 55, no. 5 (2019): 23-29.
- [GANYE 2025] Ganye, Derrick, and Kane Smith. "Examining the effects of cognitive load on information systems security policy compliance." *Internet Research* 35, no. 1 (2025): 380-418.

[GARTNER 2023a ] Gartner. "Gartner Identifies the Top Cybersecurity Trends for 2023: Security Leaders Must Pivot to a Human-Centric Focus to Establish an Effective Cybersecurity Program." 2023.

<https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023>

[GARTNER 2023b] Gartner. "CIOs need to address culture, people and process change in dynamic environments." 2023.

[GARTNER 2024] Gartner. "3 Steps to Boost Trust in Organizational Culture." 2024. <https://www.gartner.com/en/documents/5645191>

[HADLINGTON 2017] Hadlington, Lee. "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours." *Heliyon* 3, no. 7 (2017).

[HANEY 2024a] Haney, Julie, 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) at NDSS*. 2024.

[HANEY 2024b] Haney, Julie, 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.

[HINSON 2003] Hinson, John M., Tina L. Jameson, and Paul Whitney. "Impulsive decision making and working memory." *Journal of Experimental Psychology: Learning, Memory, and Cognition* 29, no. 2 (2003): 298.

[HUANG 2024] Huang, Wenjing, Sasha Romanosky, and Joe Uchill. Beyond Technicalities: Assessing Cyber Risk by Incorporating Human Factors. In *23rd Workshop on the Economics of Information Security*. 2024.

[HULL 2017] Hull, James L. "Analyst burnout in the cyber security operation center-CSOC: A phenomenological study." PhD diss., Colorado Technical University, 2017.

[JACOBS 2023] Jacobs, Jody L., Julie M. Haney, and Susanne M. Furman. "Measuring the effectiveness of U.S. government security awareness programs: A mixed-methods study." In *International Conference on Human-Computer Interaction*, pp. 14-33. Cham: Springer Nature Switzerland, 2023.

[JEONG 2019] Jeong, Jongkil, Joanne Mihelcic, Gillian Oliver, and Carsten Rudolph. "Towards an improved understanding of human factors in cybersecurity." In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, pp. 338-345. IEEE, 2019.

[KANIA 2011] Kania, John, and Mark Kramer. Collective Impact. *Stanford Social Innovation Review*, Winter 2011.

[KARADEMAS 2003] Karademas, Evangelos C., and Anastasia Kalantzi-Azizi. "The stress process, self-efficacy expectations, and psychological health." *Personality and Individual Differences* 37, no. 5 (2004): 1033-1043.

[KATCHER 2024] Katcher, Samantha, Liana Wang, Caroline Yang, Chloé Messdaghi, Michelle L. Mazurek, Marshini Chetty, Kelsey R. Fulton, and Daniel Votipka. "A Survey of Cybersecurity {Professionals} Perceptions and Experiences of Safety and Belonging in the Community." In *20th Symposium on Usable Privacy and Security (SOUPS 2024)*, pp. 1-20. 2024.

[KIM 2024] 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.

[LEE 2023] 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.

[LOVIBOND 1995] Lovibond, Peter F., and Sydney H. Lovibond. "The structure of negative emotional states: Comparison of the Depression Anxiety Stress Scales (DASS) with the Beck Depression and Anxiety Inventories." *Behaviour Research and Therapy* 33, no. 3 (1995): 335-343.

[MCLOUGHLIN 2021] McLoughlin, Ella, David Fletcher, George M. Slavich, Rachel Arnold, and Lee J. Moore. "Cumulative lifetime stress exposure, depression, anxiety, and well-being in elite athletes: A mixed-method study." *Psychology of Sport and Exercise* 52 (2021): 101823.

[MCEWEN 1993] McEwen, Bruce S., and Eliot Stellar. "Stress and the individual: Mechanisms leading to disease." *Archives of Internal Medicine* 153, no. 18 (1993): 2093-2101.

[MODIC 2012] Modic, David, and Stephen EG Lea. "How neurotic are scam victims, really? The big five and Internet scams." *The Big Five and Internet Scams (September 10, 2012)* (2012).

[MOYA 2022] Moya, Ernest, Leila M. Larson, Robert C. Stewart, Jane Fisher, Martin N. Mwangi, and Kamija S. Phiri. "Reliability and validity of depression anxiety stress scale (DASS)-21 in screening for common mental disorders among postpartum women in Malawi." *BMC Psychiatry* 22, no. 1 (2022): 352.

[NCA 2025] National Cybersecurity Alliance and Cybsafe (2025). "Oh, Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2024-2025." <https://www.staysafeonline.org/articles/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-2024>

[NOBLES 2022] Nobles, Calvin. "Stress, burnout, and security fatigue in cybersecurity: A human factors problem." *Holistica Journal of Business and Public Administration* 13, no. 1 (2022): 49-72.

[NOBLES 2023] Nobles, Calvin. "Human Factors in Cybersecurity: Academia's Missed Opportunity." In *Proceedings of the Midwest Association for Information Systems (MWAIS)*. 2023.

[NSTC 2023] 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>

[OINAS-KUKKONEN 2018] Oinas-Kukkonen, Harri, and Marja Harjumaa. "Persuasive systems design: key issues, process model and system features 1." In *Routledge Handbook of Policy Design*, pp. 87-105. Routledge, 2018.

[PAPPA 2024] Pappa, Tim, and Mike Ross. "Characterizing A NATO Cyber Victimology: A Futurist Anticipated Shame Cyber Attacker Model." NATO Veterans. 2024 <https://nato-veterans.org/characterizing-a-nato-cyber-victimology-a-futurist-anticipated-shame-cyber-attacker-model/>

[RAYWOOD-BURKE 2023] Raywood-Burke, George. "Cognitive load and subjective time pressure: How contextual factors impact the quality of cybersecurity decision making." PhD diss., Cardiff University, 2023.

[REEVES 2021] Reeves, A., P. Delfabbro, and D. Calic. "Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue." *SAGE open* 11, no. 1 (2021): 21582440211000049.

[SCHNEIER 2015] Schneier, Bruce. *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2015.

[SCHEIN 2010] Schein, Edgar H. *Organizational Culture and Leadership*. Vol. 2. John Wiley & Sons, 2010.

[SHENG 2023] Sheng, Nan, Chunjiang Yang, Lei Han, and Min Jou. "Too much overload and concerns: Antecedents of social media fatigue and the mediating role of emotional exhaustion." *Computers in Human Behavior* 139 (2023): 107500.

[SLAVICH 2014] Slavich, George M., and Michael R. Irwin. "From stress to inflammation and major depressive disorder: a social signal transduction theory of depression." *Psychological Bulletin* 140, no. 3 (2014): 774.

[SPEELMAN 2019] 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.

[SPITALETTA 2021] Spitaletta, Jason A., and Johns Hopkins. "Cyberpsychology: Adapting a Special Operations Model for Cyber Operations." (2021).

[STANTON 2016] Stanton, Brian, Mary F. Theofanos, Sandra Spickard Prettyman, and Susanne Furman. "Security fatigue." *IT Professional* 18, no. 5 (2016): 26-32.

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

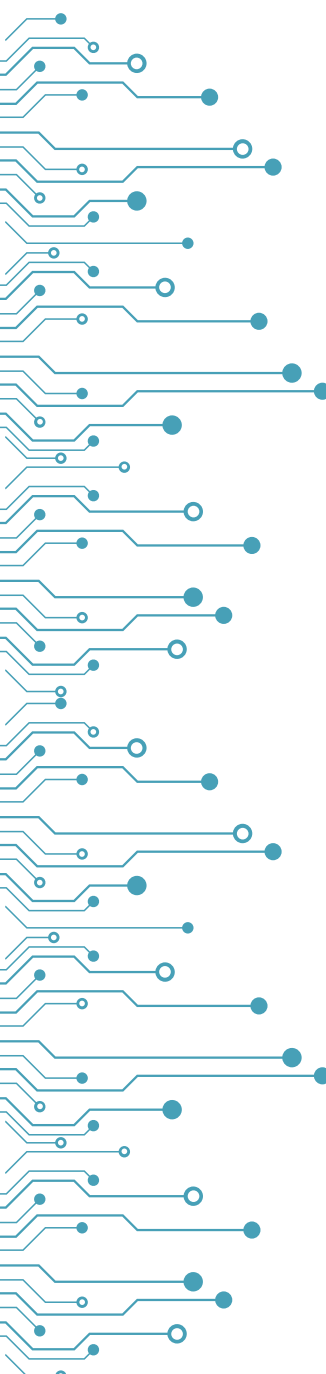
[SULER 2004] Suler, John. "The online disinhibition effect." *Cyberpsychology & Behavior* 7, no. 3 (2004): 321-326.

[SYRJAMAKI 2024] Syrjämäki, Alekski H., Mirja Ilves, Thomas Olsson, Joel Kiskola, Poika Isokoski, Anna Rantasila, Gary Bente, and Veikko Surakka. "Online disinhibition mediates the relationship between emotion regulation difficulties and uncivil communication." *Scientific Reports* 14, no. 1 (2024): 1-11.

[THOMSON 2024] Thomson, Robert, and Christian Lebiere. "Comparing Similarity and Homophily-Based Cognitive Models of Influence and Conformity." In *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*, pp. 47-57. Cham: Springer Nature Switzerland, 2024.

[VERIZON 2024] Verizon. "2024 Data Breach Investigations Report." 2024. <https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf>

[WANG 2012] Wang, Jingguo, Tejaswini Herath, Rui Chen, Arun Vishwanath, and H. Raghav Rao. "Phishing susceptibility: An investigation into the processing of a targeted spear phishing email." *IEEE Transactions on Professional Communication* 55, no. 4 (2012): 345-362.



[YENG 2022] Yeng, Prosper Kandabongee, Muhammad Ali Fauzi, and Bian Yang. "A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals." *Information* 13, no. 7 (2022): 335.

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

[ZIMMERMANN 2024] Zimmermann, Verena, Lorin Schöni, Thierry Schaltegger, Benjamin Ambuehl, Melanie Knieps, and Nico Ebert. "Human-Centered Cybersecurity Revisited: From Enemies to Partners." *Communications of the ACM* 67, no. 11 (2024): 72-81.



## CONTACT US:

<https://csrc.nist.gov/projects/human-centered-cybersecurity>  
[human-cybersec@nist.gov](mailto:human-cybersec@nist.gov)

