AUTHOR PREPRINT VERSION

# Towards Integrating Human-Centered Cybersecurity Research Into Practice: A Practitioner Survey

Julie M. Haney, Clyburn Cunningham IV, and Susanne M. Furman
National Institute of Standards and Technology
{julie.haney, clyburn.cunningham, susanne.furman}@nist.gov

***Abstract*—The "research-practice gap" can prevent the application of valuable research insights into practice. While the gap has been studied in several fields, it is unclear if prior findings and recommendations apply to human-centered cybersecurity (HCC), which may have its own challenges due to the unique characteristics of the cybersecurity field. Overcoming the gap in HCC is especially important given the large role of human behavior in cybersecurity outcomes. As a starting point for understanding this potential gap, we conducted a survey of 152 cybersecurity practitioners. We found that, while participants see the value in and are eager to receive and integrate HCC insights, they experienced a number of challenges in doing so. Based on our results, we discuss implications of our results, including how we extend prior research-practice work, suggestions for how to better support practitioners in integrating HCC into their work, and foundations for future work to explore meaningful solutions.**

## I. Introduction

The disconnect between researchers and practitioners, known as the "research-practice gap," is a well-known phenomenon that impacts myriad fields of study. This gap potentially disservices researchers and practitioners alike. Researchers may not benefit from practitioner insights that can inform the development and execution of research that is meaningful and actionable to practitioners. Conversely, practitioners may not benefit from research insights that can help guide their work and improve both their own and their users' experiences [15]. Ultimately, these shortfalls may reduce the impact of scientific research on practice.

Little work has been done to explore the research-practice gap in the interdisciplinary human-centered cybersecurity (HCC) field. HCC, often called "usable security," involves a consideration of influences on people's understanding of and interactions with cybersecurity technologies, processes, and services[39], [52]. The field's relevance and importance are grounded in the observation that many cybersecurity challenges can ultimately be attributed to people's perceptions and behaviors. For example, an industry analysis revealed that 74% of all cybersecurity breaches involve the human element (e.g., human error and social engineering) [69]. A 2023 study reported that a substantial number of people feel frustrated or intimidated by cybersecurity, do not have access to cybersecurity training, or are overwhelmed by the cybersecurity information they receive [50]. Moreover, year after year, it is reported that many organizations struggle to build meaningful programs and strategies to engage and empower their employees to make sound cybersecurity decisions [59].

To combat these trends and reduce cybersecurity failures, the technology research and consulting firm Gartner maintains that taking a human-centric approach to cybersecurity is essential, asserting that, by 2027, 50% of large enterprise CISOs will move towards adopting human-centric security design practices [28]. The guidance and information to facilitate HCC adoption is often based on evidence found by the HCC research community. Thus, there is a need to ensure the researcher and practitioner communities are adequately connected to facilitate integration of research evidence into practice.

Researchers from diverse disciplines have investigated the research-practice gap, finding that it often stems from the differing incentives, values, and work routines across the two groups [8], [12], [13]. These differences result in barriers – for example, language and format of research papers, relevance and timeliness of research, and actionability of research recommendations – that may hinder practitioners from transforming research evidence into informed action [3], [15].

It is currently unclear if research-gap issues and potential solutions identified in other fields are applicable to HCC. While the cornerstone of HCC is the well-developed discipline of human-computer interaction (HCI), the application of HCI to cybersecurity may present additional challenges [27]. For example, cybersecurity is often cited as being a unique field due to the impacts of rapidly evolving technology and threats, the adversarial setting, and the sociotechnical implications [19], [23], [27], [55].

To examine a potential disconnect in HCC, it is important to understand the perspectives of both HCC researchers and the practitioners who could make use of research insights. This paper takes the first step by exploring the practitioner perspective. We conducted an anonymous, online survey of 152 practitioners to understand their HCC perceptions, challenges, and experiences. More specifically, we sought to answer the following research questions:

**RQ1:** What are practitioners' perceptions of and experiences with HCC information in their work?
**RQ2:** How do practitioners currently and prefer to receive HCC information, if at all?
**RQ3:** What are practitioners' perceptions of HCC research?
**RQ4:** How, if at all, do HCC perceptions, experiences, and ways of receiving HCC information differ depending on

Symposium on Usable Security and Privacy (USEC) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-5-2
https://dx.doi.org/10.14722/usec.2024.23xxx
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

AUTHOR PREPRINT VERSION

prior experience as a researcher and years of experience?

**RQ5:** What HCC topics do practitioners think are most important to research?

Since practitioners may obtain HCC information from various sources and may not know whether that information has been informed by research, we started by exploring practitioners' perceptions, experiences, and barriers about HCC in general. We then, more specifically, moved to perceptions of information they know to be from HCC research. We found that, while our survey participants saw the value in and are eager to receive HCC information, they experienced challenges integrating HCC into their work, including lack of awareness of HCC concepts, organizational support, and resources. There are also gaps in how they currently receive HCC information and how they would prefer to receive it. Furthermore, participants generally viewed HCC research favorably, but a substantial number found the research difficult to find and not up-to-date with current issues and technologies. Differences among demographic groups were minimal and most often observed in how participants receive HCC information. Lastly, when asked what HCC topics were most important for researchers to focus on, participants often mentioned topics – such as security awareness training, secure development, and social engineering – that are already represented in a substantial research body of knowledge. This finding perhaps illuminates a disconnect related to existing research not reaching practitioners.

Our study makes several contributions. We extend prior research-practice gap work into the field of cybersecurity, and uniquely, human-centered cybersecurity. Our novel results provide researchers and other science communicators with insights into potential channels for disseminating research as well as ideas for research topics of most relevance to practitioners. Additionally, we provide suggestions towards informing the development of solutions that may result in greater integration of HCC into practice while alleviating undue burden on either community. Finally, our study provides a foundation of inquiry for future research opportunities that can more deeply explore and build upon our quantitative results.

## II. Related Work

The research-practice gap involves the oft-observed phenomenon of scientific research results being largely ignored by practitioners and researchers not exploring problems of value to practitioners [12]. In this section, we summarize prior work in this space related to barriers and recommendations relevant to our study's practitioner focus. We then describe how a potential gap in the human-centered cybersecurity field may be different given the unique attributes of cybersecurity.

### A. Barriers

Exploration of the research-practice gap in fields such as business management (e.g., [3], [8], [11]), conservation biology [41], social work [20], and human-computer interaction (e.g., [6], [15], [32]) reveal common barriers that hinder practitioners from using research to guide their practice. The lack of translation of research publications to practitioner-appropriate communications is a particularly glaring issue. Researchers accustomed to an academic style of writing often struggle to present their research in a form and language in which practitioners, who may not be familiar with research methodology, can understand and be willing to engage [3], [11], [15]. Practitioners are often overwhelmed by current business activities, so may not have time to seek out and read long research papers [11]. Additionally, practitioners may not be able to access research papers behind academic publication paywalls [15]. Researchers, on the other hand, may have little incentive to translate their research publications into practitioner-friendly formats or may lack the knowledge or resources to do so [8], [12], [15], [20], [41]

Practitioners want externally validated research with direct relevance to and usefulness in practice [10]. However, some research may fail to make a strong value proposition, leaving practitioners without a clear understanding of what research might have to offer them [45]. Historically long time spans to get research published are incompatible with practitioner timelines and lead to quickly outdated publications [3], [15]. Further, research outputs may lack concrete takeaways and recommendations that are actionable in the practice context [3], [6], [15]. This is often the case with abstract or theoretical research, which rarely has direct impact on practice since theories can be difficult to grasp, costly to transition to implementation, and have unclear benefits of integrating theory into practice [10], [29]. Additionally, since many researchers emphasize generalizability, they may not address transferability to the diverse contexts in which practitioners work, leaving practitioners without a pathway for implementation [13].

Beyond research outputs, lack of two-way communication between researchers and practitioners throughout the research lifecycle may lead to inaccurate or incomplete abstractions of practice and research topics that do not meet practitioners' immediate needs [3]. For example, in the HCI field, researchers' lack of understanding of design practice may be a core reason why practitioners do not show interest in new methods developed by researchers [32]. Additionally, while practitioners may have ideas about problems that need solving, these ideas are rarely communicated to researchers because there are few vehicles for them to do so [3], [6], [15], [32].

### B. Bridging the Gap

There have been a number of recommendations to help bridge the research-practice gap. Several researchers proposed formalization and frameworks related to knowledge translation ("a dynamic and iterative process that includes synthesis, dissemination, exchange, and ethically sound application of knowledge" [41]) and translational science ("the study of scientific knowledge progression from academia to practice and back" [16]). For greater impact, researchers are encouraged to present research in a form and language that practitioners can comprehend and ensure the knowledge is relevant, timely, and applicable [3], [5], [8], [54], [63]. An HCI research group suggested that researchers should move beyond a singular focus on user-centered design towards adoption-centered design [13]. This approach emphasizes the establishment of a clear value proposition for the research, not just for end users, but also for other stakeholders such as target customers, administrators, regulators, analysts, and decision-makers [13].

These proposed solutions often put the majority of the burden of knowledge transfer on researchers. However, there is

AUTHOR PREPRINT VERSION

debate about whether this should be the case, especially if researchers lack credibility with the target audience, knowledge translation skills and experience, institutional incentives, or resources [34], [41]. Consequently, supporters of translational science acknowledge that responsibility extends beyond the research and practice communities [16]. *Boundary spanners*, who serve as a bridge between scientists and non-scientists to produce outputs that enable communication between the two groups, could relieve researchers from translation and transfer tasks they are not trained for and are reluctant to do. [41], [58]. Formal *evidence bridges* – independent intermediaries between science and practice that translate research findings into the language of practice while also translating the needs of practitioners into issues researchers can address – may also aid in knowledge exchange [41]. For example, evidence bridges in the field of medicine – such as the American Cancer Society, Royal College of Physicians and Surgeons, and the Canadian Pediatric Society – "engage with medical practitioners, synthesize primary research relevant to decision making, and make evidence easily accessible" [41].

### C. Application to Human-Centered Cybersecurity

*1) Why Human-Centered Cybersecurity May Be Different:* While the research-practice gap has been identified in multiple fields – including the closely related HCI discipline – we posit that considerations and solutions to the gap in HCC may be different than many other fields because of the unique nature of the cybersecurity field itself. This difference has been observed when applying other research fields to the cybersecurity context, for example, industrial and organizational psychology [24] and artificial intelligence [55].

From a practitioner perspective, cybersecurity is unique in several ways. First, the intangible, uncertain nature of cybersecurity – including vulnerabilities, impacts, possible victims, and hackers – can hinder the ability of organizations and individuals to effectively assess security risks in advance [19]. This may result in lack of action since risk may be mistakenly viewed as unlikely or only a remote possibility [62].

Second, cybersecurity is subject to a rapid pace of change, with threats, technologies, and regulations constantly evolving [23], [24], [55]. The cybersecurity solutions of today may not be relevant tomorrow [49], so keeping up with the latest developments can be overwhelming for both cybersecurity experts and non-experts alike [19], [23], [48], [60].

Third, unlike many disciplines, cybersecurity involves adversaries who interfere with stakeholders' goals [48], [55]. Beyond malicious actors, the very beneficiaries of cybersecurity (i.e., end users) or those tasked with implementing it may be viewed as "enemies" or "the weakest link" [2], [33], [62], [70]. Consequently, the "human in the loop" is often regarded as a problem to be controlled rather than empowered [71].

A fourth unique attribute of cybersecurity is the uncertainty and debate about which cybersecurity solutions are most effective [60]. Because cybersecurity can never be completely guaranteed, it may be difficult to justify return on investment and demonstrate success [19], [23] Moreover, proposed solutions may result in tensions, for example, cybersecurity vs. individual privacy [19] or usability [24].

Finally, and perhaps most relevant to HCC, cybersecurity requires a sociotechnical approach involving multiple disciplines and the interplay between human, social, organizational, technical, and broader community factors [19], [49], [55]. However, technological solutions and approaches still dominate the cybersecurity community, with many cybersecurity practitioners not understanding the intricacies of the relationships critical to success in the field [37]. Practitioners are put at a disadvantage from the start of their professional education and training due to an "emphasis on technical and engineering skills while discounting the important social and organizational influences that dictate success or failure in everyday settings" [18].

*2) Cybersecurity Studies:* There has been little exploration of the research-practice gap in cybersecurity, let alone in HCC. One study found that popular cybersecurity research topics do not always coincide with practitioners' main concerns [22]. Others recommended that research teams involve cybersecurity subject matter experts early in the research to ensure developed technology is responsive to organizational needs [30]. A human-centric research study suggested that it is not the case that security decision makers do not care or are ignorant about the impact research findings may have [56]. Rather, they simply do not know how to apply research findings.

Different from these studies, our initial approach to exploring the research-practice gap more broadly focuses on practitioners' perceptions of HCC and challenges integrating HCC insights into practice. We believe this is a first step in informing the research community and knowledge transfer intermediaries so that research evidence is more relevant, available, and consumable to practitioners.

## III. Methodology

We conducted an anonymous, online survey of 152 practitioners to explore practitioners' perceptions of and experiences with HCC. We opted to conduct a survey since we had a strong foundation for developing survey questions and responses based on prior qualitative interview and case studies related to the research-practice gap ([11], [13], [15], [22], [61]).

### A. Survey Development

Our research questions and findings from prior studies informed our initial draft of survey questions and answer options. Further, the experiences of our interdisciplinary research team contributed to crafting the survey. Our three-person team had over 25 years combined practitioner experience in cybersecurity and software development and over 30 years combined research experience in human factors psychology, human-computer interaction, and human-centered cybersecurity.

Two subject matter experts reviewed the initial draft to check for alignment with the research questions, clarity, and completeness. Both reviewers had extensive experience designing surveys for HCC research, and one had prior practitioner experience as a software developer and program manager for systems requiring high levels of cybersecurity. We incorporated their suggestions into the final survey.

To ensure participants understood what was meant by HCC, we described the concept at the beginning of the survey.

AUTHOR PREPRINT VERSION

Currently, there is no standard definition for human-centered cybersecurity, nor the related terms "usable security" and "sociotechnical security" [67]. Therefore, we created a composite description based on explanations from other research groups that work in this space [52], [39], [35], [68]. We provided the following description to survey participants:

> *Human-centered security (sometimes called "usable security") considers the human, social, and organizational factors related to security processes, technologies, products, policies, etc. It involves the relationships and interactions between people and cybersecurity, including people's perceptions, the challenges they encounter, and designing usable systems, products, and services that also result in improved security outcomes.*

The final survey (included in Appendix A) consisted of select-one-option, select-all-that-apply, Likert scale, and open-ended response questions. We examined perceived importance of integrating HCC insights into work practice, the current and preferred ways of receiving research evidence, perceptions of HCC research, and the challenges in accessing, digesting, and utilizing HCC insights. We further provided practitioners the opportunity to suggest human-centered research topics that would be of most value to them. There were also survey questions that collected basic professional demographic and organizational characteristics of participants.

### B. Data Collection and Participants

Eligible survey participants had to be adults (18+ years of age) with jobs involving developing, administering, implementing, or overseeing cybersecurity-related resources (e.g., technologies, systems, processes, policies) or the cybersecurity components of those resources. This description was provided in the recruitment materials to establish criteria for participation and represent the wide range of practitioners who could benefit from receiving HCC information. To recruit practitioners, we advertised the study via cybersecurity practitioner mailing lists and social media posts (X and LinkedIn) from accounts primarily followed by practitioners and sent email invitations to professional contacts.

The survey, implemented on the Qualtrics platform, was open for three weeks in July 2023. We reviewed the data to eliminate partial responses and check for response patterns that may indicate poor data quality. We included a total of 152 practitioner survey responses in the final data set.

Table I shows participant demographics. The largest percentage of participants identified at least one of their roles as security practitioner (63%), followed by manager/executive (32%). About 38% of participants had 10 or fewer years of experience in the cybersecurity field. Over half worked in private industry organizations, with government being the next most represented organization type. Over three-quarters worked for organizations in North America.

We also asked about prior experiences with cybersecurity research. Forty-one percent either had conducted research in the past or were currently researchers. Over half had provided input during the conceptualization, design, or analysis of a research study or been a participant in a cybersecurity-related research study. Furthermore, just under 40% had presented at a conference or event primarily attended by researchers, with most of those having done so from a practitioner perspective.

TABLE I. PARTICIPANT DEMOGRAPHICS (N = 152)

| Demographic | Response Option | n | % |
|---|---|---|---|
| Practitioner role | Security practitioner | 95 | 62.50% |
| | Manager/executive | 48 | 31.58% |
| | IT practitioner | 28 | 18.42% |
| | Educator/trainer | 27 | 17.76% |
| | Policy maker | 16 | 10.53% |
| | Developer | 12 | 7.89% |
| | Other | 11 | 7.24% |
| Years of experience | Less than 1 | 7 | 4.61% |
| | 1 to 5 | 21 | 13.82% |
| | 6 to 10 | 29 | 19.08% |
| | 11 to 15 | 28 | 18.42% |
| | 16 to 20 | 20 | 13.16% |
| | More than 20 | 47 | 30.92% |
| Organization type | Academic | 19 | 12.50% |
| | Private industry | 88 | 57.89% |
| | Non-profit | 9 | 5.92% |
| | Government | 32 | 21.05% |
| | Other | 4 | 2.63% |
| Region | Africa | 1 | 0.66% |
| | Asia | 7 | 4.61% |
| | Europe | 17 | 11.18% |
| | North America | 123 | 80.92% |
| | Oceania | 2 | 1.32% |
| | South America | 1 | 0.66% |
| | Caribbean Islands | 0 | 0.00% |
| | Pacific Islands | 1 | 0.66% |
| Prior researcher experience | Yes, past | 33 | 21.71% |
| | Yes, current | 29 | 19.08% |
| | No | 90 | 59.21% |
| Provided input to a research study | Yes | 83 | 54.61% |
| | No | 69 | 45.39% |
| Been a research study participant | Yes | 76 | 50.33% |
| | No | 75 | 49.67% |
| Given a presentation at a security research event | Yes, practitioner perspective | 52 | 34.21% |
| | Yes, researcher perspective | 16 | 10.53% |
| | No | 92 | 60.53% |

### C. Data Analysis

We calculated descriptive statistics and inferential statistics using Stata statistical software to look for significant ($\alpha = 0.05$) differences across the data. We also employed qualitative methods to analyze responses from the two open-ended questions.

*1) Statistical Analysis:* We explored differences based on practitioner demographics by comparing independent groups for two variables with the most potential of influence on responses. We postulated that prior or current ***researcher experience*** might influence the ways in which participants find, use, and perceive HCC information and research. We were also interested in ***years of experience*** since those with longer practitioner work histories may have had more opportunity for on-the-job exposure to human element issues and information.

For greater power in our statistical analysis, we combined several demographic groups for the variables of interest. Researcher experience consisted of two groups: those with prior or current experience as a researcher (n = 62) and those without researcher experience (n = 90). For years of experience, we collapsed categories of 10 or less years into an "less experience" group (n = 57) and those with more than 10 into a "more experience" group (n = 95).

We used Mann Whitney U tests to compare responses for ordinal data (Likert scales), reporting significant results with the z-statistic. For categorical question responses (selecting/not

AUTHOR PREPRINT VERSION

TABLE II. EFFECT INDICES AND SIZE THRESHOLDS

| Index | Test | Small | Medium | Large |
|---|---|---|---|---|
| **Independent groups** | | | | |
| Cohen's d (d) [14] | Mann-Whitney U | 0.20 | 0.50 | 0.80 |
| Cramer's V (V) [43] | Chi square (1 deg freedom), Fisher's exact | 0.10 | 0.30 | 0.50 |
| **Matched data** | | | | |
| Effect size (r) [53] | Wilcoxon signed-rank | 0.10 | 0.30 | 0.50 |
| Odds ratio (OR) [46] | McNemar's | 1.22 (0.538, 0.82] | 1.86 (0.333, 0.538] | 3.00 [0.33, $\infty$) |

selecting an option), we used Chi-square tests of association – reported with $\chi^2$ and degrees of freedom (df) – or Fisher's exact tests in instances of five or less occurrences [43].

We also explored the data for significant differences in matched (paired) data. In the case of comparisons for ordinal response data (e.g., whether there was a difference between ratings of HCC research being understandable vs. being easy to find), we utilized the Wilcoxon signed rank test (reported with the z-statistic). For categorical responses (e.g., differences between current and preferred methods of receiving HCC information), we used McNemar's test (reported with $\chi^2$).

For each significant statistical result, we also report the effect size to show the magnitude of the difference. A large effect size may indicate that a finding has practical significance, while a small effect size may indicate limited practicality [64]. In Table II, we summarize our methods of calculating effect size for each type of statistical test as well as the thresholds for small, medium, and large effect sizes.

*2) Open-ended Question Data Analysis:* We analyzed the data from the open-ended survey questions using qualitative coding techniques. There were 108 responses to a question about barriers to incorporating HCC into practice, averaging 23 words per response. A question about HCC topics of interest yielded 104 responses averaging 27 words. For each question, two researchers individually read through the responses and developed an initial set of codes. They then met to discuss their codes, agree upon a codebook, and operationalize (clearly define and describe) each of the codes. The same two researchers then independently coded all responses using the codebook, coming back together again to resolve coding conflicts. As recommended by qualitative methodologists, we placed emphasis on insights reached during our coding discussion rather than calculating agreement statistics [47], [4]. Codes were then grouped into higher level categories, which are presented in our results. The final codebook for responses related to barriers (reported in IV-B-2) is included in Appendix B. Table IV displays the codebook for responses about HCC topics.

### D. Ethics

The study was approved by our institutional review board. The survey's first screen provided participants with information about the study purpose, procedure, the voluntary nature of the survey, their rights as a participant, and how their data would be protected. Advancement past this first screen indicated participant consent. Survey responses were collected anonymously and assigned participant IDs (e.g., P22). Identifiable information entered in open-ended survey responses was redacted from the research record. Participants were not compensated.

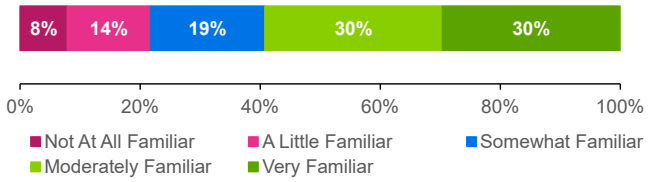


Fig. 1. Degree of familiarity with concept of human-centered cybersecurity

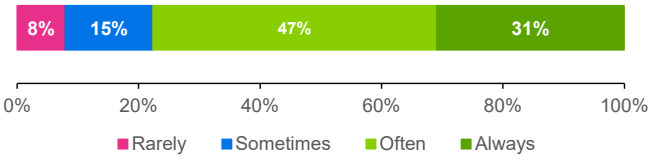


Fig. 2. How often participants consider human-centered cybersecurity in their work

## IV. RESULTS

We report our survey findings with descriptive statistics and significant inferential statistical results. Research question 1 (RQ1), related to perceptions of and experiences with HCC, is addressed in sections IV-A and IV-B. Section IV-C contains results for RQ2, how practitioners receive HCC information. Results about perceptions of HCC research (RQ3) are reported in section IV-D. Differences among demographics groups (research experience and years of experience) are reported throughout these sections. Finally, RQ4, concerning research topics of importance, is addressed in section IV-E.

### A. Perceptions of Human-Centered Cybersecurity

We asked participants a series of questions to understand their experiences with and thoughts related to HCC in general.

*1) Familiarity with Human-Centered Cybersecurity:* Survey participants rated their familiarity with HCC on a 5-point scale ranging from "not at all familiar" to "very familiar" (Fig. 1)[1]. Over half (59%) said they were moderately or very familiar with HCC, with only 8% saying that they were not familiar. There were no significant differences for researcher experience or years of experience.

*2) Frequency of Considering Human-Centered Cybersecurity:* Participants indicated the frequency with which they considered aspects of HCC in their work on a 5-point scale ranging from "never" to "always" (Fig. 2 ). HCC was often or always considered by 78% of survey participants, with no participants indicating that they never consider it. There were no significant differences for the variables of interest.

*3) Importance of Human-Centered Cybersecurity:* We asked participants to rate the level of importance of considering HCC in their work on a 5-point scale ranging from "not important" to "extremely important" (Fig. 3). Most (91%)

[1]Percentages in figures depicting Likert scale responses are rounded to the nearest whole number.

AUTHOR PREPRINT VERSION

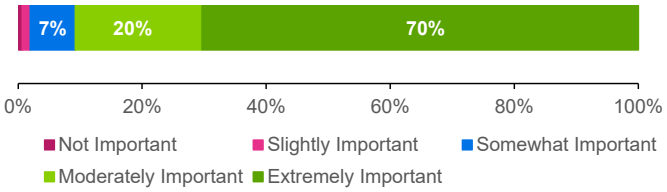


Fig. 3. Participants' ratings of the importance of considering human-centered cybersecurity in their work

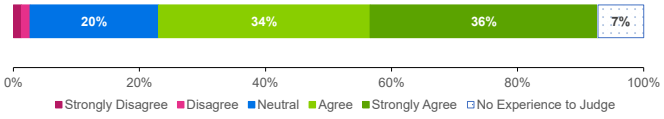


Fig. 4. Agreement with the statement "Information about human-centered security has made a positive impact on my work."

selected moderately or extremely important. More experienced career participants rated HCC as significantly more important than those with less experience (z = -2.70, d = 0.40).

*4) Positive Impact of HCC:* Participants also rated their level of agreement with the statement: "Information about human-centered security has made a positive impact on my work" on a 5-point scale ranging from "strongly disagree" to "strongly agree" with an additional "no experience to judge" option (Fig. 4). A majority (70%) either agreed or strongly agreed with the statement, while less than 3% disagreed or strongly disagreed. About 7% selected "no experience to judge." Excluding "no experience to judge" responses in the statistical tests, we found no significant differences for the two variables of interest.

### B. Challenges When Considering HCC

We explored challenges practitioners face when considering HCC in their daily work by asking them to rate their level of challenge, then describe their challenges.

*1) Challenge Rating:* Participants rated the level of challenge they experience when considering HCC in their work on a 5-point scale ranging from "not challenging" to "extremely challenging" with a "no experience to judge" option (Fig. 5). Although many participants had rated HCC as important and frequently-considered in their work, 76% nonetheless found the consideration to be moderately or extremely challenging. Inferential statistical tests (excluding "no experience to judge") found no significant differences for the variables of interest.

*2) Barriers:* We asked participants an open-ended question "What are the barriers to you, as a practitioner, being able to integrate human-centered security into your work?" From the 108 responses, we identified six overarching themes.

**Awareness and knowledge.** Lack of awareness and knowledge about HCC was mentioned as a barrier by 36 participants. On a basic level, some practitioners may not consider HCC because there is a "Perception that security is a technology issue, and not human-centered" (P141). A participant working in the government sector noted this barrier as "Understanding (many

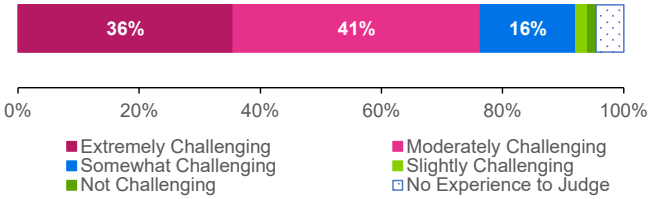


Fig. 5. Level of challenge participants experience when considering human-centered cybersecurity in their work

don't really understand the taxonomy of human involvement so it's hard to focus others from whatever their incoming mental models were)" (P138). An educator/trainer working in private industry wrote that practitioners are not trained in HCC: "[Human-centered security is] not basic of IT/cybersecurity education... It would take longer time and supportive resource for awareness" (P86).

Even if there is awareness, some practitioners may lack the knowledge to take action. An industry practitioner mentioned "lack of knowledge by stakeholders (clients and auditors)" (P148). Several participants admitted their own lack of knowledge in this area. For example, one participant expressed they were "not sure where to start" (P56), and another said, "I don't know what I don't know" (P73).

**Organizational support and change.** Lack of organizational support and acceptance (mentioned by 20 participants) was cited as a barrier to integrating HCC into practice. Commonly, this deficiency originated from leadership specifically. For example, a security practitioner in an academic institution described the barrier simply as "lack of commitment from top levels of the organization to make this a priority" (P69). Lack of support can also come from customers, as illustrated by an IT practitioner who mentioned, "There is a lack of value placed on involvement from companies we work for to include a human element to security operations" (P103).

Organizational staff members, especially participants' own cybersecurity practitioner peers, may not support HCC integration because of "change resistance" (P93) (mentioned by 10 participants). One participant noted a challenge of "Fighting against outdated mindsets and security team culture that end users or business/non tech people are not treated with the respect they deserve as professionals and teams" (P144). Another responded that a barrier is "people's resistance to see the user as an all[y]" (P104).

Lack of support and resistance to change are often grounded in a weak value proposition for HCC. Having to "very clearly be able to articulate the value and the process" (P53) can be daunting. A security practitioner commented that the "disruption of introducing cybersecurity controls, protocols and policies is already a tough sell. There's some basic understanding and concern for the protection provided by these controls, protocols and policies that is required before it becomes a value proposition." (P67). The introduction of HCC into these controls, protocols, and policies faces similar challenges. Convincing organizations of the value of HCC is made even more difficult when practitioners cannot cite concrete evidence that HCC improves cybersecurity. An industry

AUTHOR PREPRINT VERSION

security practitioner cited "providing objective evidence that the solution lives up to the promises" as a challenge (P27). A government IT practitioner wrote, "critical reflections on the application of HCD [human-centered design] are lacking" (P54). A participant working in private industry believed there was a lack of credible research:

> "Not enough substantiated, verifiable, credible research documentation that cites sources and provides access to research data and methodology, to the extent possible, so that the conclusions presented in the research could be recalculated to confirm or refute the conclusions from an independent and objective standpoint" (P75)

**Resources.** The lack of awareness and absence of organizational support, particularly among leadership, often manifests itself in lack of resources (mentioned by 37), including funding, staff, and time. A participant described this barrier simply as "Resources (seen as nice to have not essential)" (P138). An industry security practitioner and policy maker stated, "Personnel in organizations may not be aware of the value of human-centered security, and therefore don't understand, have confidence in, or allocate time or resources to it" (P44).

In addition, practitioners are simply quite busy, so may not have the time to dedicate to learning about and integrating HCC. For example, a participant cited a barrier as the "Timeframe required to do the research and implementation" (P17). A manager/executive working in private industry said, "this is not an area that I have been officially tasked with researching so most of what I have learned has been on my own time" (P125). A government security and IT practitioner wrote that "practitioners often are not given the time to work as closely with the people performing the business/research processes as they need to" (P133).

**Guidance.** HCC standards and guidance might help overcome insufficient awareness and knowledge of HCC. However, 14 participants thought these resources were lacking. For example, one practitioner cited a barrier being "Lack of generally accepted and widely known principles and recommendations for practitioners" (P15). Further, HCC concepts may not be integrated into cybersecurity standards and guidance, which may lead to a de-emphasis of the value of HCC. A government participant blamed the technical focus of widely-used guidance: "Lack of a comprehensive framework that includes human-centered security aspects with the technical aspects. The current RMF [Risk Management Framework [52]], while vast and broad, really devolves to policy and technical vs the human-centered security interactions" (P26). To progress towards more inclusion of HCC considerations, another participant recommended, "I believe there needs to be a bridge to include psychology based expertise in addition to security SMEs [subject matter experts] when considering creation or adding an addendum to standards, frameworks that include this human centered security" (P118).

Problematically, guidance does not always reflect the state-of-the-art in HCC. A participant remarked that there was "Not enough info on current topics of concern, information tends to be old/out of date" (P61). A lack of current information is particularly concerning when included in policies. For example, a participant said a barrier was "Audit requirements for outdated practices or controls (e.g., password complexity vs. passphrases). We know things about human behaviour yet continue to apply policies that do not align" (P151).

**Tools and technology.** Tools, systems, and other technologies may not aid practitioners in integrating HCC (mentioned by 18 participants). A practitioner in private industry commented on the lack of consideration of HCC when developing technical solutions: "Technology workflows do not support or involve the human aspect or context. Technology is treated as a dumb tool, e.g., a hammer. It's time to build better tools with human-centric security built in" (P117). Another wrote that there is "little ability to change or be flexible in the controls or options to make them more usable to humans" (P70)

In addition, few tools help identify HCC issues. A developer commented on the focus on technical cybersecurity risks within automated tools: "We now rely on tools to identify any security risks, and if the automated tool does not find it, it must not be a problem" (P115). Another participant cited the "Lack of industry leading tools that incorporate human-centered security into their product offering. Difficult to custom build it into existing solution offerings" (P127).

**Users.** Nine participants described the lack of motivation and knowledge of organizational employees (users) as a barrier to integrating HCC in their work. One participant commented on lack of motivation: "others not taking security seriously" (P30). Moreover, users may not understand cybersecurity or their responsibility for it. As P41 stated, "The people who need the most knowledge are often uninterested, at least initially. Alternatively, they're overwhelmed by the idea of cybersecurity." A security practitioner working in private industry commented that "Convincing users of the importance of their roles in recognizing vulnerabilities and reporting suspicious events" (P100) is a barrier. A government practitioner noted, "Our challenge is engaging employees and users, so they recognize and respond proactively" (P34).

### *C. Receiving Human-Centered Cybersecurity Information*

Participants selected the means through which they currently become aware of HCC topics and insights and, in a later question, how they prefer to receive HCC information. Fig. 6 shows the response percentages for both current and preferred. In addition to the items in the figure, 5% of participants indicated that they are not aware of these topics (current) and one participant indicated that they do not care to learn about HCC (preferred).

Over half of participants *currently* become aware of HCC topics and insights via: discussions with colleagues; papers or articles in practitioner-focused publications; websites, blogs, and online forums; and presentations at practitioner conferences or events. Participants with research experience more often selected discussions with researchers ($\chi^2$ = 16.04, V = 0.32), papers/articles in research-focused publications ($\chi^2$ = 8.01, V = 0.23), and presentations at research conferences/events ($\chi^2$ = 16.04, V = 0.32) as compared to participants without research experience. Less-experienced participants less often selected social media ($\chi^2$ = 4.13, V = 0.16) and tools (Fisher's exact p = 0.045, V = 0.17) compared to their more-experienced counterparts.

AUTHOR PREPRINT VERSION

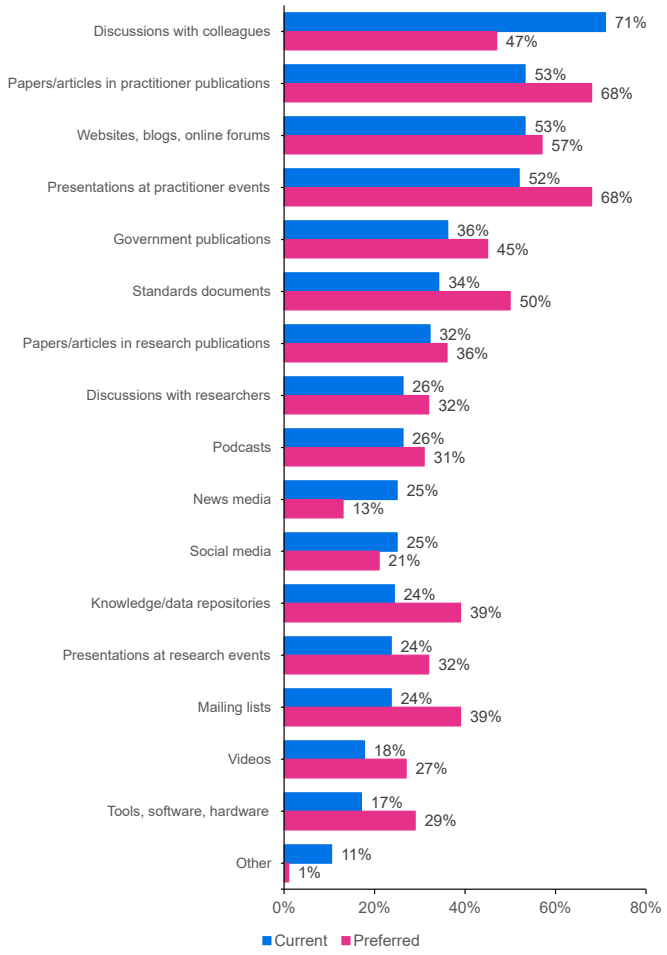


Fig. 6. Ways in which participants currently and prefer to obtain human-centered cybersecurity information

*Preferences* for these same avenues differed in magnitude. At least half preferred to receive HCC information via: papers or articles in practitioner-focused publications; presentations at practitioner conferences or events; websites, blogs, and online forums; and standards documents. Participants with research experience more frequently selected discussions with researchers ($\chi^2$ = 5.90, V = 0.20), papers/articles in research publications ($\chi^2$ = 8.51, V = 0.24), and presentations at research conferences/events ($\chi^2$ = 5.90, V = 0.20). Those with research experience less often selected websites ($\chi^2$ = 4.07, V = 0.16). Less-experienced participants more often selected mailing lists compared to those with more cybersecurity experience ($\chi^2$ = 4.26, V = 0.17).

We further found that gaps between current and preferred means of obtaining information were significant for most options, with medium or large effect sizes. As compared to current means, participants had a statistically significant *preference* for receiving information via papers/articles in practitioner-focused publications ($\chi^2$ = 27.0, OR = 7.0), presentations at practitioner conferences/events ($\chi^2$ = 11.0, OR = 0.33), presentations at researcher conferences/events ($\chi^2$ = 5.12, OR = 0.44), videos ($\chi^2$ = 5.12, OR = 0.44), mailing lists ($\chi^2$ = 13.71, OR = 0.27), tools ($\chi^2$ = 8.40, OR = 0.39), knowledge/data repositories ($\chi^2$ = 11.76, OR = 0.32), government publications ($\chi^2$ = 4.33, OR = 0.50), and standards documents ($\chi^2$ = 11.26, OR = 0.34). Participants preferred to receive *less* information via discussions with colleagues ($\chi^2$ = 27.0, OR = 7.0) and news media ($\chi^2$ = 8.53, OR = 2.80) than they currently do.

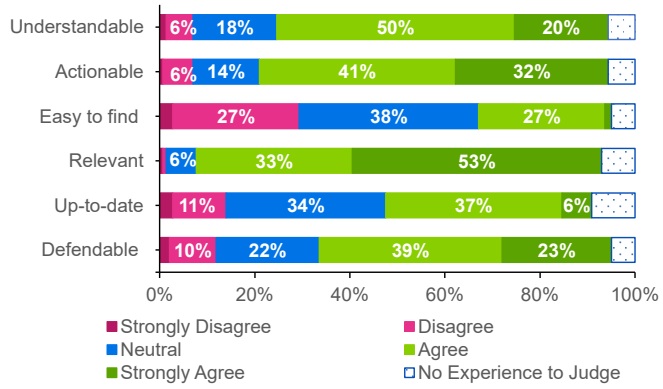


Fig. 7. Agreement that attributes apply to human-centered cybersecurity research

### D. Perceptions of Human-Centered Cybersecurity Research

Recognizing that participants may receive HCC information from a variety of sources, we wanted to specifically explore their perceptions of HCC *research*. In the survey, we provided a definition of formal HCC research to differentiate it from the generic "insights" and "information" referred to in the rest of the survey: "a systematic investigation (e.g., a survey, interview, or experimental study) to explore the human, social, and organizational aspects of security."

*1) Attribute Ratings:* We asked participants to rate their level of agreement on a 5-point scale with a "no experience to judge" option about whether they think six attributes apply to HCC research. Attributes included: understandable; actionable (worded as "something I can take and put into action"); easy to find ("easy to find and access"); relevant ("relevant to my organization or situation"); up to date ("up to date with current issues and technologies"); and defendable ("defendable to peers and leadership within my organization"). This question was not presented to the 5% who indicated that they were not aware of HCC topics, as reported in section IV-C.

Fig. 7 shows the ratings. Participants most often agreed that HCC research is relevant (85%), actionable (73%), and understandable (70%). Participants least often agreed that it is up to date (43%) and easy to find (28%). We did not find any significant differences for the variables of interest. Applying a Holm-Bonferroni correction to adjust for multiple comparisons [1], we did, however, find significant differences between ratings for all attribute pairs except understandable and defendable (see Table III). Easy to find and up to date had lower agreement ratings than all other attributes. All but one significant pairwise comparison (understandable and actionable) had medium or large effect sizes.

*2) Interest:* We asked participants to rate their level of interest in receiving information about HCC research on a 5-point scale ranging from "not interested at all" to "extremely

AUTHOR PREPRINT VERSION

TABLE III. SIGNIFICANT PAIRWISE COMPARISONS OF HUMAN-CENTERED CYBERSECURITY RESEARCH ATTRIBUTE RATINGS

| Attribute Pair | z | Effect Size (r) |
|---|---|---|
| Understandable - actionable | -2.37 | 0.21 |
| Understandable – easy to find | 7.91 | 0.69 |
| Understandable-relevant | -6.57 | 0.58 |
| Understandable – up to date | 4.50 | 0.40 |
| Actionable – easy to find | 8.40 | 0.73 |
| Actionable - relevant | -4.75 | 0.42 |
| Actionable – up to date | 5.63 | 0.49 |
| Actionable – defendable | 2.55 | 0.22 |
| Easy to find – relevant | -9.38 | 0.82 |
| Easy to find – up to date | -3.80 | 0.33 |
| Easy to find – defendable | -6.36 | 0.55 |
| Relevant – up to date | 8.03 | 0.72 |
| Relevant – defendable | 6.56 | 0.58 |
| Up to date – defendable | -4.09 | 0.36 |

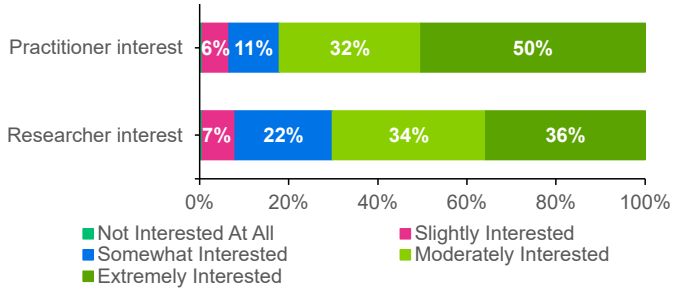


Fig. 8. Participants' own interest in receiving information about human-centered cybersecurity and perceived researcher interest in producing research outputs for practitioners

interested." To glean their perceptions about the research community's motivation, we also asked participants to rate their perceptions of how interested HCC researchers would be in producing research output for practitioners like them. Fig. 8 shows the ratings for both questions. Over three-quarters (82%) of participants said they would be moderately or extremely interested in receiving HCC research information. Significantly fewer, but still a majority (70%), believed that researchers would be moderately/extremely interested in producing output for them ($z = 3.76$, $r = 0.31$). We did not find any statistically significant differences for the variables of interest.

### E. Research Topics

We asked practitioners an open-ended question about which HCC topics they think are most important to research. Table IV provides an overview of the 104 responses. Security awareness training was the most popular topic area. Three other topic areas were mentioned by at least 25% of respondents: security operations and administration; governance, policy, and compliance; and social engineering and media.

Note that, in the survey, we provided examples in the question to help guide practitioners' understanding of what might constitute an HCC research topic. However, given that some participants simply referenced the examples in their responses, we acknowledge the limitations of the response data for this question. For transparency, we indicate topic areas for which specific topic examples were included with an asterisk (*) in Table IV. For example, since the example of phishing was in the survey, we highlight its potential influence on the higher-level "Social engineering and social media" topic. Despite this limitation, many participants included their own topics or provided more details related to the example topics. Furthermore, participants' inclusion of the example topics may indeed signify areas of most interest or concern. Therefore, there is still value in reporting this data.

## V. DISCUSSION

Our study is a novel investigation of the research-practice gap within the human-centered cybersecurity field from the practitioner perspective. In this section, we situate our research results within existing literature, provide practical recommendations for supporting practitioners, and suggest future research opportunities.

### A. Advancing Research-Practice Gap Knowledge

*1) Perceptions and Barriers:* Overall, participants had positive perceptions of HCC and HCC research, with most finding it to be important and impactful and believing that HCC researchers want to produce outputs for them. These results are surprising as they are in contrast to other research-practice gap studies that found practitioners often view research as hard to understand and not actionable, and do not believe researchers are motivated to produce outputs specifically for them [3], [5], [11], [15]. Part of this discrepancy may be due to the formats in which our participants receive HCC information, some of which may have already been tailored to practitioner needs and not in their original research paper formats.

Despite these positive perceptions, our survey uncovered areas of concern. Participants generally did not believe HCC research to be easy to find or access, an observation previously noted [15]. Participants also often indicated that HCC research was not up to date with current issues and technologies, a result consistent with practitioner perceptions in HCI design practice studies [3], [15]. However, we acknowledge that the practitioner sources from which participants commonly receive HCC information may be – unbeknownst to practitioners – examples of translated research.

We further discovered that our practitioner participants tended to experience a high level of challenge integrating HCC into their work. Other literature uncovered similar challenges for practitioners when applying research, such as difficulty understanding specialized research terminology and concepts, not feeling confident in the research topics, lack of translation into practitioner tools and processes, having little time, and resistance to change [11], [13], [15].

*2) Uniqueness of the Cybersecurity Field:* We see evidence that the nature of cybersecurity may impact perceptions and experiences perhaps differently than in other fields. Fields previously studied in the research-practice context – such as HCI design practice [12], [15], conservation biology [41], and management [3], [11] – tend to be slow to change. In contrast, the rapid pace of change in cybersecurity [23] may result in practitioners believing that HCC research that is even just a few years old is outdated. This assumption may contribute to the frustration our participants shared about how cybersecurity guidance, policies, and standards move at a much slower pace, potentially resulting in outdated recommendations incorporating the state-of-the-art in HCC. The constant evolution in the field may also result in practitioners simply not having the time to actively look for HCC information (with time constraints

AUTHOR PREPRINT VERSION

TABLE IV. HUMAN-CENTERED CYBERSECURITY RESEARCH TOPICS OF MOST IMPORTANCE TO PARTICIPANTS (% OUT OF 104 RESPONSES)

| Topic Area | Examples | n | % |
|---|---|---|---|
| Security awareness and training* | · "Making folks aware of why these things really should matter to them and making any training contextually significant to their role(s) in the organization." (P69)<br>· "training and awareness at the executive and board levels" (P105)<br>· "education at middle school, high-school, and undergraduate college-level curriculum that requires courses focused on living securely in an internet delivered world." (P135) | 44 | 42% |
| Incident response and security operations* | · "Operating guidance for folks in an adaptive zero trust environment…without confusing people" (P10)<br>· "Most effective methods…to identify when something has likely gone wrong (when prevention/avoidance fails), and to respond promptly and effectively to contain spread and reduce losses when things go wrong." (P15)<br>· "Organization, leadership, and individual dynamics during the detection, response, and mitigation of an incident that develops into a serious breach" (P107) | 33 | 32% |
| Governance, policy, and compliance* | · "policy effectiveness and compliance" (P31)<br>· "Effective but EFFICIENT security policy…i.e., target the key risk areas and incorporate awareness of personnel time when going farther down the priority list." (P59)<br>· "Enforceable / actionable security guidelines and compliance." (P108) | 32 | 31% |
| Social engineering and social media* | · "We need to validate if phishing training in its current form is more harm than help" (P81)<br>· "general cyber-hygiene especially with regard to Social Media." (P67)<br>· "Practical strategies for work to prepare employees for social engineering attacks that are up to par with new technologies (i.e., Chat GPT, Cloud, etc.)" (P107) | 28 | 27% |
| Authentication* | · "improved authentication understanding/usability" (P126)<br>· "Pervasive implementation of passwordless protocols and authentication mechanisms. With a heavy dose of thought around how non-technical users implement and recover from loss of access." (P14)<br>· "Understanding the importance of secure authentication methods" (P141) | 24 | 23% |
| Workforce development* | · "cybersecurity workforce development" (P03)<br>· "secure software development in all Computer science higher-education courses" (P135) | 23 | 22% |
| Secure development* | · "DevSecOps" (P116)<br>· "developers: usable and automated mechanisms for implementation" (P62)<br>· "How can we make developing secure software to be perceived as desirable and interesting than developing a great feature?" (P92) | 23 | 22% |
| User behaviors and attitudes | · "psychological safety" (P80)<br>· "Understanding risk-taking behaviors by senior leadership" (P107)<br>· "Why people resist security controls, seeing it as an inconvenience despite the protections they provide" (P127) | 23 | 22% |
| Organizational culture | · "How to develop a practical culture of security that balances organizational value with the costs, time, and effort require[d]." (P44)<br>· "executive buy-in in theory but in practicality it seems to be largely ignored" (P105)<br>· "how to change the culture in order to minimize cyber incidents" (P13) | 8 | 9% |
| Risk management | · "Research into adapting policy to an organization's current threat perspective." (P77)<br>· "How people think about cybersecurity risk management" (P52)<br>· "insider risk" (P80) | 6 | 6% |
| Communication | · "how to communicate effectively during a cyber incident." (P13)<br>· "Working on making terminology more understandable." (P41)<br>· "how to explain cybersecurity risks and countermeasures to people that are not working in a technical area" (P76) | 5 | 5% |
| Measurement and benchmarking | · "cybersecurity self-assessments to bring to bear peer measurement within organizations so people can judge where they fall within the market" (P45)<br>· "the human cost of cyber crime" (P47)<br>· "how to measure the human dimension of cybersecurity. If you can't measure it, you can't improve it." (P119) | 5 | 5% |
| Data protection | · "data loss prevention" (P70)<br>· "data management and security" (P105)<br>· "digital footprint" (P80) | 3 | 3% |
| Other topics | · "supply chain" (P83)<br>· "standardization of human-centered security" (P96)<br>· "cloud security adoption" (P97)<br>· "Scenario-based experimentation in cyber ranges" (P119)<br>· "The role of AI/ML in this field" (P128) | 8 | 8% |

* indicates a topic area for which a related example was provided in the survey

noted in our results) or HCC information being lost in the volume of security information they receive.

Further divergences from previously-studied fields were evident in participants' comments about the adversarial relationship between cybersecurity practitioners and employees/users, which is in contrast to how users are viewed in related fields such as HCI [27], [62]. This finding may also be related to practitioners' de-emphasis of critical sociotechnical factors and often-singular focus on technology. The lack of awareness and knowledge of HCC mentioned by our participants may be attributed, in part, to the phenomenon that cybersecurity practitioners are missing a piece of their education, as most are not trained in non-technical aspects of the field [18], [37].

Uncertainty about the effectiveness of cybersecurity solutions was reflected in participant responses about difficulties providing a value proposition for HCC and gaining organizational support. Determining return on investment (ROI) of cybersecurity solutions is already acknowledged as challenging [19], [23]. Establishing a value proposition and proving ROI of human-element security measures (e.g., training) may be even harder because organizations are frequently not capturing human-centric measures of effectiveness [40], as evidenced by participants' desire for more research on measurement.

*3) Receiving HCC Information:* We uniquely identify significant gaps in how practitioners currently and prefer to receive HCC information. Participants' preference for practitioner publications and forums is a potential signal that they want HCC information to be integrated into their current information sources and workflows. Interestingly, participants most often reported discussions with colleagues as a way in which they obtain HCC information. This may be because practitioners traditionally find value in learning about others' experiences [15] or they do not know where else to get this information. Ultimately, this finding leads to questions about the credibility and validity of peer-provided information

AUTHOR PREPRINT VERSION

and whether other, more credible sources might be preferred. Indeed, when asked about preferences, participants selected colleague discussions significantly less often. In addition, there was a decrease in preference for receiving information via the news media, which has recently experienced a decrease in public trust [26]. Although participants remarked that HCC was not well-integrated into guidance publications, policies, or standards, the substantial preference for HCC information to be delivered via these channels may demonstrate a desire to receive information through official or authoritative channels. Future research efforts could further explore the idea of source credibility among cybersecurity practitioners.

### *B. Supporting Practitioners, Bridging the Gap*

Our participants saw the importance of human-centered cybersecurity and were eager to receive and apply HCC research insights. Based on our results and grounded in supporting literature, we offer suggestions for how practitioners can better be supported in accomplishing this integration.

**Encourage institutions and individuals to serve as bridges.** The HCC field may benefit from the creation of evidence bridges between researchers and practitioners [41] to address the negative perceptions of research findability and currency found in our study (section D). A bridge could synthesize and translate research for practitioners who could apply research insights to improve people's interactions with cybersecurity. In addition, bridges could offer practitioners a channel for providing researchers with their uniquely qualified insights on HCC research topics having the most potential for practical impact and how research-informed solutions perform and offer a value proposition in the real world [15].

Since evidence bridges are typically independent intermediaries between the communities, we raise the question of which organizations are most qualified, trusted by both communities, and best positioned to serve as evidence bridges. There may be a role for government research funding organizations (e.g., U.S. National Science Foundation, European Research Council, and Natural Sciences and Engineering Research Council of Canada) to facilitate their funded projects having real-world impact. Trusted non-profits might also be candidates.

Individuals and organizations can also be full- or part-time, formal or informal boundary spanners. Science communicators and others skilled in translating research information to practitioner language can share curated research evidence, as also suggested by other researchers [16], [61], in ways preferred by practitioners (section C). Practitioners with experience and connections in both communities (so-called "pracademics" [54]) could serve as a bridge since, as our survey supported (section C), they more often keep abreast of HCC in research-focused venues. Organizations that employ both researchers and practitioners could also be a bridge. For example, one such organization created a public research library containing HCC resources [17]. This type of data/knowledge repository was desired by a substantial number of survey participants and could provide practitioners with a central location to search for information on topics of most interest.

**Share information via channels practitioners are likely to use.** To address the finding that participants think HCC research is difficult to find and access (section D), we suggest that HCC information be primarily disseminated through the practitioner-focused channels (e.g., publications, conferences/events, websites/blogs/online forums, mailing lists) they prefer and already use. This approach of "pushing" information rather than expecting practitioner to "pull" (i.e. seek out information on their own) respects practitioners' limited time – a barrier mentioned in the survey (section B-2) and consistent with past research about cybersecurity practitioners being overwhelmed [9], [25]. Taking this approach, we offer several suggestions for how research can be communicated to practitioner audiences.

Some practitioner cybersecurity conferences encourage talks related to HCC. For example, the popular conferences RSA [57] and Black Hat [7] feature human element/human factors tracks. However, the tracks are typically dominated by practitioners and vendors, some of whom may present information not well-grounded in research evidence. Researchers may be hesitant to present at these conferences as travel funds may be hard to secure. Therefore, conference sponsors could consider offering grants to attract researchers to these events.

To avoid travel altogether, trusted cybersecurity organizations in the public and private sectors could offer periodic webinars on HCC topics, interview researchers for podcasts, or include mentions of HCC insights in their mailing list announcements. Publishers of practitioner-focused magazines and newsletters could include articles grounded in HCC research. Scientific research publishers can provide articles or special issues geared towards practitioners or provide better search tools and open access to help practitioners find applicable research. We note, however, that survey participants without research experience infrequently preferred to receive HCC from researcher-focused publications and events (section C). Therefore, depending on potential reasons for not engaging with these forums (e.g., subscription pay wall, lack of awareness, disinterest in research formats), attempts to increase access to pure academic research forums may not be fruitful in increasing practitioner exposure to HCC research.

To support the desire of participants to receive HCC information in government publications and standards documents (section C), we encourage the developers of these documents to include considerations for the human-element (e.g., usability, equity, and communications). It should also be communicated that these considerations are critical towards assuring cybersecurity adoption and success. As an example, the widely-used Special Publication 800-63 Digital Identity Guidelines from the U.S. Government includes considerations for usability and stresses the importance of limiting user burden [51].

Our findings also reveal potential targeting strategies for practitioners at different stages of their careers (section C). We see the importance of disseminating teasers of HCC information via social media for more-established practitioners. These individuals have likely developed more extensive professional networks and are more likely to interact on professional social media platforms such as LinkedIn [66]. Conversely, less-experienced participants prefer HCC information be pushed to them via mailing lists, perhaps indicating a reluctance to search for the information on their own.

**Distill basic HCC principles and benefits.** The fundamental

deficiencies in awareness, knowledge, and appreciation for the value proposition of HCC lead to limited organizational support and resources (section B). To address these challenges, we suggest that researchers, evidence bridges, and boundary spanners engage in the creation and widespread distribution of easily-consumable information on basic HCC principles and the importance of HCC in cybersecurity practice. HCC primers could be in several forms. Professional training courses about HCC basics or integration of HCC concepts into existing professional certification programs could provide a formalized pathway to learning about HCC. Further, the need to impart the importance of HCC earlier in people's careers may be supported by our finding that less experienced survey participants rated the importance of HCC significantly lower than more experienced participants. Thus, we see the need for more integration of human-centered computing concepts into traditional computer science and related degree programs.

A second possibility could entail short, targeted publications that distill HCC concepts discovered through research into a format more digestible to practitioners and disseminated through practitioner venues. For example, an article "Eight Lightweight Usable Security Principles for Developers" [31] was published in a magazine and then succinctly summarized in a one-page website targeted at developers [38]. Advertised via mailing lists and social media, a U.S. government agency published a two-page handout describing common human-element misconceptions and suggestions for how to overcome those [36]. HCC basics could also include tips on communicating to non-technical audiences and decision makers, a topic of interest among the survey participants. Guidance for communicating during specific cybersecurity situations (e.g., in the midst of cyber incidents [44]) could also be valuable.

**Prioritize the synthesis and reporting of research topics of most importance to practitioners.** We note that there is a large, existing body of research knowledge in several of the topic areas listed by participants in section E, for example security awareness and training (e.g., [42]), social engineering (e.g., [21]), and secure development (e.g., [65]). This may imply that practitioners are not aware of the research. Therefore, our findings identify areas of priority for synthesis and presentation to practitioners. Researchers and boundary spanners could produce meta-analyses, literature reviews, or other evidence syntheses that include research evidence on these topics (as suggested by [3]). These compendiums may be more valuable and palatable to busy practitioners. In addition, because these represent the results from multiple research efforts, they may hold up better to scrutiny as compared to single studies.

### C. Limitations and Opportunities for Future Work

Our study has several limitations. As is common in self-report studies with nonprobablity sampling, there may be self-selection bias. Participants who opted to complete the survey may have had a pre-existing interest in HCC, which could explain the high percentages of participants indicating that they were familiar with HCC or viewed it as important.

Several demographic skews may also limit the wide applicability of our results. Our participants largely worked in North American institutions, likely because of the U.S.-based mailing lists used for recruitment. Therefore, it is unclear as to whether our results apply to practitioners in other regions. In addition, a substantial number of participants had prior research experience. To account for this, we utilized inferential statistics to determine when this prior experience influenced responses. Not surprisingly, prior research experience influenced how participants received HCC information, biasing them more towards research publications and forums. However, these significant differences may have limited practicality due to their small effect sizes. Interestingly, we note that research experience did not translate into significantly different views on HCC research or any other perception or experience.

Finally, we acknowledge that, although a sizeable research community works on cybersecurity projects related to developers (e.g., [31], [33], [65]), less than 8% of our participants held this role. Since developers may work under different pressures and incentives than other practitioners, we see the value of a similar survey being conducted with developers to better inform the developer-centered research community.

There are opportunities to build upon our study. Our largely quantitative results provide insights into practitioner ratings but offer few explanations into the reasons behind participants' responses nor solutions that would be most valuable to practitioners without requiring extensive effort on their part. A follow-up study with practitioners to gather in-depth, qualitative responses could fill these gaps. Additionally, it is important to explore the researcher perspective to discover potential areas of conflict and harmony between the two communities. We leave this exploration to future work.

## VI. Conclusion

Through a survey of 152 cybersecurity practitioners, we begin to uncover perceptions, experiences, and challenges that could enable or hinder the critical application of human-centered cybersecurity research into practice. Our study adds to the current research body of knowledge by exploring a field with unique characteristics and challenges as compared to previously-studied fields. Based on our results, we provide researchers, boundary spanners, and cybersecurity guidance producers with suggestions on how to more effectively disseminate HCC information to practitioners. We also uniquely capture which HCC research topics are of most interest to practitioners, providing a roadmap for priority areas warranting synthesis and future research. These insights can help progress the integration of evidence-based HCC concepts and actions into cybersecurity practice, resulting in better outcomes for individuals and organizations.

## Disclaimer

Certain commercial companies or products are identified in this paper to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.

## Acknowledgements

We would like to thank Steven Furnell and Mary Theofanos who provided valuable feedback on the study design and the

AUTHOR PREPRINT VERSION

anonymous reviewers whose suggestions helped improve this paper. We would also like to thank the practitioners who took time from their busy schedules to thoughtfully complete the survey.

## REFERENCES


[1] H. Abdi, "Holm's sequential bonferroni procedure." *Encyclopedia of research design*, vol. 1, no. 8, pp. 1–8, 2010.

[2] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[3] C. Bailey, "Employee engagement: Do practitioners care what academics have to say–and should they?" *Human Resource Management Review*, vol. 32, no. 1, p. 100589, 2022.

[4] R. S. Barbour, "Checklists for improving rigour in qualitative research: a case of the tail wagging the dog?" *British Medical Journal*, vol. 322, no. 7294, pp. 1115–1117, 2001.

[5] J. M. Bartunek and S. L. Rynes, "Academics and practitioners are alike and unlike: The paradoxes of academic–practitioner relationships," *Journal of Management*, vol. 40, no. 5, pp. 1181–1201, 2014.

[6] J. Beck and H. R. Ekbia, "The theory-practice gap as generative metaphor," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–11.

[7] Black Hat, "Black hat briefing tracks," https://www.blackhat.com/html/tracks.html, 2023.

[8] I. Bleijenbergh, J. van Mierlo, and T. Bondarouk, "Closing the gap between scholarly knowledge and practice: Guidelines for HRM action research," *Human Resource Management Review*, vol. 31, no. 2, p. 100764, 2021.

[9] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, "Studying IT security professionals: research design and lessons learned," in *Position paper for the CHI Workshop on Security User Studies: Methodologies and Best Practices*, 2007.

[10] D. M. Boyle, J. F. Boyle, and D. R. Hermanson, "How to publish in peer-reviewed practitioner accounting journals," *Issues in Accounting Education*, vol. 35, no. 2, pp. 19–30, 2020.

[11] K. Božič, A. A. Bachkirov, and M. Černe, "Towards better understanding and narrowing of the science–practice gap: A practitioner-centered approach to management knowledge creation," *European Management Journal*, vol. 40, no. 4, pp. 632–644, 2022.

[12] E. Buie, S. Dray, K. Instone, J. Jain, G. Lindgaard, and A. Lund, "How to bring HCI research and practice closer together," in *CHI'10 Extended Abstracts on Human Factors in Computing Systems*, 2010, pp. 3181–3184.

[13] P. K. Chilana, A. J. Ko, and J. Wobbrock, "From user-centered to adoption-centered design: a case study of an HCI research innovation becoming a product," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 1749–1758.

[14] J. Cohen, "A power primer," *Psychological Bulletin [PsycARTICLES]*, vol. 112, no. 1, pp. 155–159, 1992.

[15] L. Colusso, C. L. Bennett, G. Hsieh, and S. A. Munson, "Translational resources: Reducing the gap between academic research and HCI practice," in *Proceedings of the 2017 Conference on Designing Interactive Systems*, 2017, pp. 957–968.

[16] L. Colusso, R. Jones, S. A. Munson, and G. Hsieh, "A translational science model for HCI," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–13.

[17] CybSafe, "Research library," https://www.cybsafe.com/research-library/, 2023.

[18] J. Dawson and R. Thomson, "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance," *Frontiers in Psychology*, vol. 9, p. 744, 2018.

[19] H. deBruijn and M. Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," *Government Information Quarterly*, vol. 34, no. 1, pp. 1–7, 2017.

[20] V. Denvall and M. Skillmark, "Bridge over troubled water—closing the research–practice gap in social work," *The British Journal of Social Work*, vol. 51, no. 7, pp. 2722–2739, 2021.

[21] G. Desolda, L. S. Ferro, A. Marrella, T. Catarci, and M. F. Costabile, "Human factors in phishing attacks: a systematic literature review," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–35, 2021.

[22] G. Dhillon, K. Smith, and I. Dissanayaka, "Information systems security research agenda: Exploring the gap between research and practice," *The Journal of Strategic Information Systems*, vol. 30, no. 4, p. 101693, 2021.

[23] K. Doyle, Z. Dooly, and P. Kearney, "What's so unique about cyber security?" in *Cyber Security and Privacy: 4th Cyber Security and Privacy Innovation Forum, CSP Innovation Forum 2015*. Springer International Publishing, 2015, pp. 131–139.

[24] R. C. Dreibelbis, J. Martin, M. D. Coovert, and D. W. Dorsey, "The looming cybersecurity crisis and what it means for the practice of industrial and organizational psychology," *Industrial and Organizational Psychology*, vol. 11, no. 2, pp. 346–365, 2018.

[25] J. Dykstra and C. L. Paul, "Cyber operations stress survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations," in *11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18)*, 2018.

[26] Gallup and Knight Foundation, "American views: Trust, media and democracy," https://knightfoundation.org/wp-content/uploads/2018/01/KnightFoundation_AmericansViews_Client_Report_010917_Final_Updated-2.pdf, 2018.

[27] S. Garfinkel and H. R. Lipford, *Usable security: History, themes, and challenges*. Morgan & Claypool Publishers, 2014.

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

[29] S. Geldof and J. Vandermeulen, "A practitioner's view of human–computer interaction research and practice," *Artifact: Journal of Design Practice*, vol. 1, no. 3, pp. 134–134, 2007.

[30] L. B. Goldrich, L. Davis, D. Miller, R. Gatlin, and B. Gattoni, "Embedded r&d for cybersecurity in an operational environment," in *2015 48th Hawaii International Conference on System Sciences*, 2015, pp. 5185–5191.

[31] P. L. Gorski, L. L. Iacono, and M. Smith, "Eight lightweight usable security principles for developers," *IEEE Security & Privacy*, vol. 21, no. 1, pp. 20–26, 2022.

[32] C. M. Gray, E. Stolterman, and M. A. Siegel, "Reprioritizing the relationship between hci research and practice: bubble-up and trickle-down effects," in *Proceedings of the 2014 conference on Designing interactive systems*, 2014, pp. 725–734.

[33] M. Green and M. Smith, "Developers are not the enemy!: The need for usable security APIs," *IEEE Security & Privacy*, vol. 14, no. 5, pp. 40–46, 2016.

[34] J. M. Grimshaw, M. P. Eccles, J. N. Lavis, S. J. Hill, and J. E. Squires, "Knowledge translation of research findings," *Implementation Science*, vol. 7, no. 1, pp. 1–17, 2012.

[35] M. Grobler, R. Gaire, and S. Nepal, "User, usage and usability: Redefining human centric cyber security," *Frontiers in Big Data*, vol. 4, p. 583723, 2021.

[36] J. Haney and S. Furman, "Handout: Users are not stupid: 6 cybersecurity pitfalls overturned," https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=936113, 2023.

[37] J. M. Haney, W. Lutters, and J. Jacobs, "Cybersecurity advocates: Force multipliers in security behavior change," *IEEE Security & Privacy*, vol. 19, no. 4, pp. 54–59, 2021.

[38] Hochschule Bonn-Rhein-Sieg and Universität Bonn, "Usable security principles for developers and their end-users," https://www.usablesecurityprinciples.dev/, 2023.

[39] International Computer Science Institute, "Usable security and privacy," https://www.icsi.berkeley.edu/icsi/groups/privacy, 2022.

[40] J. L. Jacobs, J. M. Haney, and S. M. Furman, "Measuring the effectiveness of us government security awareness programs: A mixed-methods study," in *International Conference on Human-Computer Interaction*, 2023, pp. 14–33.

[41] A. N. Kadykalo, R. T. Buxton, P. Morrison, C. M. Anderson, H. Bickerton, C. M. Francis, A. C. Smith, and L. Fahrig, "Bridging research

AUTHOR PREPRINT VERSION

and practice in conservation," *Conservation Biology*, vol. 35, no. 6, pp. 1725–1737, 2021.

[42] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Computers & Security*, vol. 106, p. 102267, 2021.

[43] H.-Y. Kim, "Statistical notes for clinical researchers: Chi-squared test and fisher's exact test," *Restorative Dentistry & Endodontics*, vol. 42, no. 2, pp. 152–155, 2017.

[44] R. Knight and J. R. Nurse, "Effective communications and public relations after a cyber security incident," https://jasonnurse.github.io/comms.pdf, 2020.

[45] N. Kumar and N. Dell, "Towards informed practice in hci for development," *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, pp. 1–20, 2018.

[46] S. S. Mangiafico, "Summary and analysis of extension program evaluation in r, version 1.20.05," https://rcompanion.org/handbook/, 2023.

[47] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice," in *ACM on Human-Computer Interaction*, 2019, p. 72.

[48] D. McMorrow, "Science of cyber-security," https://apps.dtic.mil/sti/pdfs/ADA534220.pdf, The MITRE Corporation, Tech. Rep., 2010.

[49] L. Metcalf and J. Spring, *Using Science in Cybersecurity*, 2021.

[50] National Cybersecurity Alliance and Cybsafe, "Oh behave! the annual cybersecurity attitudes and behaviors report 2023," https://staysafeonline.org/online-safety-privacy-basics/oh-behave/, 2023.

[51] National Institute of Standards and Technology, "Special publication 800-63 digital identity guidelines," https://pages.nist.gov/800-63-3/, 2017.

[52] ——, "Human-centered cybersecurity," https://csrc.nist.gov/projects/human-centered-cybersecurity, 2023.

[53] J. Pallant, *Survival manual: A step by step guide to data analysis using SPSS*, 4th ed., 2011.

[54] A. Panda, "Bringing academic and corporate worlds closer: We need pracademics," *Management and Labour studies*, vol. 39, no. 2, pp. 140–159, 2014.

[55] J. Paredes, J. C. Teze, G. I. Simari, and M. V. Martinez, "On the importance of domain-specific explanations in ai-based cybersecurity systems (technical report)," *CoRR*, vol. abs/2108.02006, 2021. [Online]. Available: https://arxiv.org/abs/2108.02006

[56] S. Parkin, A. V. Moorsel, P. Inglesant, and M. A. Sasse, "A stealth approach to usable security: helping IT security managers to identify workable security solutions," in *Proceedings of the 2010 New Security Paradigms Workshop*, 2010, pp. 33–50.

[57] RSA, "Rsa conference tracks," https://www.rsaconference.com/usa/call-for-submissions/tracks, 2023.

[58] H. D. Safford, S. C. Sawyer, S. D. Kocher, J. K. Hiers, and M. Cross, "Linking knowledge to action: the role of boundary spanners in translating ecology," *Frontiers in Ecology and the Environment*, vol. 15, no. 10, pp. 560–568, 2017.

[59] SANS, "Sans 2022 security awareness report: Managing human risk," https://go.sans.org/lp-wp-2022-sans-security-awareness-report, 2022.

[60] N. M. Scala, A. C. Reilly, P. L. Goethals, and M. Cukier, "Risk and the five hard problems of cybersecurity," *Risk Analysis*, vol. 39, no. 10, pp. 2119–2126, 2019.

[61] C. E. Smith, E. Nevarez, and H. Zhu, "Disseminating research news in HCI: Perceived hazards, how-tos, and opportunities for innovation," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

[62] J. D. Still, "Cybersecurity needs you!" *Interactions*, vol. 23, no. 3, pp. 54–58, 2016.

[63] A. Styhre, "The influence of neoliberalism and its absence from management research," *International Journal of Organizational Analysis*, vol. 22, no. 3, pp. 278–300, 2014.

[64] G. M. Sullivan and R. Feinn, "Using effect size—or why the p value is not enough," *Journal of Graduate Medical Education*, vol. 4, no. 3, pp. 279–282, 2012.

[65] M. Tahaei and K. Vaniea, "A survey on developer-centred security," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2019, pp. 129–138.

[66] Target Internet, "How different age groups are using social media 2023," https://targetinternet.com/resources/how-different-age-groups-are-using-social-media-2023/, 2023.

[67] M. Theofanos, "Is usable security an oxymoron?" *Computer*, vol. 53, no. 2, pp. 71–74, 2020.

[68] University of Maryland College of Information Studies, "Sociotechnical Cybersecurity (STC) Interest Group," https://ischool.umd.edu/centers-and-labs/stc/, 2023.

[69] Verizon, "2023 data breach investigations report," https://www.verizon.com/business/resources/reports/dbir, 2023.

[70] R. West, C. Mayhorn, J. Hardee, and J. Mendel, "The weakest link: A psychological perspective on why users make poor security decisions," in *Social and Human elements of Information Security: Emerging Trends and Countermeasures*, 2009, pp. 43–60.

[71] V. Zimmermann and K. Renaud, "Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset," *International Journal of Human-Computer Studies*, vol. 131, pp. 169–187, 2019.

## APPENDIX

## APPENDIX A: SURVEY INSTRUMENT

### TERMINOLOGY

***Security*** *will be used as shorthand for cybersecurity.*

***Human-centered security*** *(sometimes called "usable security") considers the human, social, and organizational factors related to security processes, technologies, products, policies, etc. It involves the relationships and interactions between people and cybersecurity, including people's perceptions, the challenges they encounter, and designing usable systems, products, and services that also result in improved security outcomes.*

### INFORMATION ABOUT YOU AND YOUR JOB

**1) Which of the following best describes your current position as a practitioner? Select all that apply. If you are also a researcher, you will have an opportunity to indicate that later in the survey.**

- ☐ Security practitioner
- ☐ IT practitioner
- ☐ Software or hardware developer
- ☐ Manager or executive
- ☐ Policy maker
- ☐ Educator or trainer
- ☐ Other (please specify)

**2) How many years have you worked in a job involving security?**

- ○ 1-5
- ○ 6-10
- ○ 11-15
- ○ 16-20
- ○ More than 20 years

**3) Which of the following best describes your current, primary organization/institution?**

- ○ Academic
- ○ Private industry
- ○ Non-profit
- ○ Government
- ○ Other (please specify)

**4) In which region is your current organization?**

- ○ Africa

- Asia
- Europe
- North America
- Oceania
- South America
- Carribean Islands
- Pacific Islands

## INVOLVEMENT WITH RESEARCH

**5) Have you ever been a researcher?**

- Yes, in the past
- Yes, and I currently still am a researcher
- No

**6) Have you ever provided input into the conceptualization, design, or analysis of a research study?**

- Yes
- No

**7) Have you ever been a participant in a security-related research study (for example, as a study interviewee, survey respondent, or participant in an experiment)?**

- Yes
- No

**8) Have you ever given a presentation at a security-related research conference or other event primarily attended by researchers?**

- Yes - from a practitioner perspective
- Yes - from a researcher perspective
- No

## HUMAN-CENTERED SECURITY

*Please answer the following questions from your practitioner perspective (even if you have been or are currently a researcher).*

*Reminder:* ***Human-centered security*** *considers the human, social, and organizational factors related to security processes, technologies, products, policies, etc. It involves the relationships and interactions between people and cybersecurity, including people's perceptions, the challenges they encounter, and designing usable systems, products, and services that also result in improved security outcomes.*

**9) How familiar are you with human-centered security?**

Not at all Familiar - A Little Familiar - Somewhat Familiar - Moderately Familiar - Very Familiar

**10) What do you think is the level of importance of considering human-centered security in your work?**

Not Important - Slightly Important - Somewhat Important - Moderately Important - Extremely Important

**11) How often do you consider aspects of human-centered security in your work?**

Never - Rarely - Sometimes - Often - Always

**12) What is the level of challenge you have experienced when considering human-centered security in your work?**

Not Challenging - Slightly Challenging - Somewhat Challenging - Moderately Challenging - Extremely Challenging - No Experience to Judge

**13) Rate your level of agreement with the following statement: "Information about human-centered security has made a positive impact on my work."**

Strongly Disagree - Disagree - Neutral - Agree - Strongly Agree - No Experience to Judge

**14) For what reasons do you disagree that human-centered security has made a positive impact on your work?** *(Only asked if Strongly Disagree or Disagree was selected in Question 13)*

**15) Through what means, if any, have you become aware of human-centered security topics and insights? Select all that apply.**

- ☐ Discussions with colleagues
- ☐ Discussions with researchers
- ☐ Papers/articles in practitioner-focused publications
- ☐ Papers/articles in research-focused publications
- ☐ Presentations at practitioner-focused conferences, meetings, or other events
- ☐ Presentations at research-focused conferences, meetings, or other events
- ☐ Podcasts
- ☐ News media
- ☐ Videos
- ☐ Websites, blogs, other online forums
- ☐ Social media
- ☐ Mailing lists
- ☐ Tools or other software or hardware
- ☐ Knowledge and data repositories
- ☐ Government publications
- ☐ Standard documents
- ☐ Other (please specify)
- ☐ I am not aware of these topics

**16) This question is about your opinions related to formal human-centered security research, which is a systematic investigation (e.g., a survey, interview, or experimental study) to explore the human, social, and organizational aspects of security. Rate your agreement with the following: "Human-centered security research is _____."** *(Only asked if "I am not aware of these topics" was NOT selected in Question 15)*

Strongly Disagree - Disagree - Neutral - Agree - Strongly Agree - No Experience to Judge

**Understandable**
**Something I can take and put into action**
**Easy to find and access**
**Relevant to my organization or situation**
**Up-to-date with current issues and technologies**
**Defendable to peers and leadership within my organization**

**17) How interested are you in receiving information about human-centered security research?**

Not Interested at all - Slightly Interested - Somewhat Interested - Moderately Interested - Extremely Interested

**18) In your opinion, what is the extent to which human-centered security researchers would be interested in producing research outputs for practitioners like you?**

Not Interested at all - Slightly Interested - Somewhat Interested - Moderately Interested - Extremely Interested

**19) Through what means, if any, would you *prefer* to receive information about human-centered security topics and insights in the future? Select all that apply.**

- ☐ Discussions with colleagues
- ☐ Discussions with researchers

AUTHOR PREPRINT VERSION

- ☐ Papers/articles in practitioner-focused publications
- ☐ Papers/articles in research-focused publications
- ☐ Presentations at practitioner-focused conferences, meetings, or other events
- ☐ Presentations at research-focused conferences, meetings, or other events
- ☐ Podcasts
- ☐ News media
- ☐ Videos
- ☐ Websites, blogs, other online forums
- ☐ Social media
- ☐ Mailing lists
- ☐ Tools or other software or hardware
- ☐ Knowledge and data repositories
- ☐ Government publications
- ☐ Standard documents
- ☐ Other (please specify)
- ☐ I don't care to learn about these topics

**20) What are the barriers to you, as a practitioner, being able to integrate human-centered security into your work?** _____

**21) What human-centered security topics do you think are most important for researchers to focus on right now (for example, how people respond to security attacks, cybersecurity workforce development, usable authentication mechanisms, phishing, security policy compliance, secure development, threat detection tools, security awareness training)?** _____

## APPENDIX B: BARRIER CODES

HCC awareness and knowledge

- Lack of awareness
- Lack of knowledge

Organizational support and change

- Acceptance and support
- Prioritization
- Resistance to change

Resources

- Funding
- Time and staff

Guidance

- HCC principles
- Integration of HCC into technical documents
- State of the art

Tools and technology

- Tool and system design and coding
- Toolsets for HCC

Users

- Motivation - taking security seriously
- Knowledge