From Fear to Control: Developing a Three-Factor Scale for Cybersecurity Anxiety (CybAS)

Nikolaj Dall
ndndall@hotmail.com
University of Southern Denmark
Odense, Denmark

Hanno Gustav Hagge
hhagg2000@gmail.com
University of Southern Denmark
Odense, Denmark

Peter Mayer
University of Southern Denmark
Odense, Denmark
Karlsruhe Institute of Technology
Karlsruhe, Germany
mayer@imada.sdu.dk

Cori Faklaris
cfaklari@charlotte.edu
University of North Carolina at Charlotte
Charlotte, USA

ABSTRACT

Cybersecurity anxiety captures the persistent worry, stress and perceived lack of control individuals experience when navigating digital threats. While prior research has examined privacy concerns, computer anxiety and related constructs, no validated instrument exists to specifically measure anxiety in cybersecurity contexts. We address this gap with the Cybersecurity Anxiety Scale (CybAS), a 15-item psychometric instrument developed through literature review, item generation, and multiple survey studies. CybAS consists of three factors: *Present* (current concerns), *Future* (anticipated threats), and *Control* (perceived control over outcomes). Analyses confirm strong reliability and validity, and the concise format makes CybAS suitable for both research and applied settings. Beyond measurement, CybAS offers HCI researchers a diagnostic framework for detecting misalignments between users' mental models and security technologies, enabling the design of anxiety-aware security systems that directly address emotional barriers, bridging the gap between usability, trust, and security.

CCS CONCEPTS

• **Human-centered computing** → **HCI design and evaluation methods**; *User studies*; • **Security and privacy** → **Usability in security and privacy**.

KEYWORDS

psychometrics, worry, stress, attitudes, emotions, paranoia, artificial intelligence, privacy

ACM Reference Format:
Nikolaj Dall, Hanno Gustav Hagge, Peter Mayer, and Cori Faklaris. 2026. From Fear to Control: Developing a Three-Factor Scale for Cybersecurity Anxiety (CybAS). In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3772318.3791187

Please use nonacm option or ACM Engage class to enable CC licenses
This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
CHI '26, April 13–17, 2026, Barcelona, Spain
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2278-3/2026/04
https://doi.org/10.1145/3772318.3791187

1 INTRODUCTION

Users constantly interact with security mechanisms, from password managers to multi-factor authentication prompts. The effectiveness of these systems depends on how well a user's mental model (their internal understanding of threats, safeguards, and consequences) aligns with the system's design [16, 75]. When this alignment fails, it can lead to more than just errors; it can foster a state of worry, stress and perceived lack of control. Moreover, individuals are increasingly exposed to cybersecurity risk as a consequence of their daily digital consumption [54]. This can affect how they perceive and interact with digital systems and create strong emotions [13, 67], leading to feelings of worry and stress [3]. These emotions toward cybersecurity, including anxiety, can impact preventive measures, compliance and behavioral intentions [76, 77], and behaviors themselves [14]. We define as *cybersecurity anxiety* this worry, stress, and perceived lack of control that individuals experience when navigating a landscape of myriad digital threats and security practices. This concept is a critical HCI concern, as it signals a fundamental disconnect between the user and the technology, leading to disengagement and unsafe behaviors [14]. If we design technologies that do not align with users' mental models or emotional states, people are unlikely to adopt or engage with them, even if the technologies are highly effective [77]. This paper introduces a tool to diagnose the amount and nature of this disconnect, enabling us to design interventions that rebuild user understanding and confidence.

Prior research has examined constructs adjacent to cybersecurity anxiety. Studies in usable security and privacy have introduced scales measuring behaviors, attitudes or resilience in relation to cybersecurity threats [2, 25, 27, 29, 45, 55]. Similarly, psychology and HCI research have developed validated scales for anxiety. This spans from clinical contexts [7, 33, 37, 70, 80], to domain specific forms such as computer anxiety [38] or artificial intelligence anxiety [78]. Privacy research has also highlighted how concerns over data collection and surveillance affect individuals' behavior and well-being [5, 34, 53]. Collectively, these studies indicate that stress and worry related to cybersecurity are complex and not fully captured by existing scales.

Despite these advances, there is still no validated scale that specifically measures anxiety related to cybersecurity threats and practices. Existing scales either target behaviors or attitudes (e.g., SeBIS [25] and SA-6 [29]), resilience (e.g., Human Cyber-Resilience Scale [45]) or more general fear and paranoia that shows a persistent thought process apart from emotion (e.g., Cyber-Paranoia and Fear Scale [55]). While these scales are valuable, they do not directly assess the emotional responses that capture cybersecurity anxiety, including worry, stress and perceived lack of control in cybersecurity contexts (as opposed to paranoia as feeling of others being out to harm you or fear that is just one of the aspects of anxiety). This gap limits the ability of researchers and practitioners to study the impact of cybersecurity threats in terms of anxiety responses by individuals, and design interventions that address the emotional consequences.

To address this gap, we present the **Cybersecurity Anxiety Scale (CybAS)**, a psychometric instrument designed not only to measure anxiety but to diagnose the underlying nature of a user's flawed mental model. Its 15-item, three-factor structure allows us to differentiate between three distinct sources of anxiety: (a) *Present Anxiety*, representing individuals' current anxiety about security threats; (b) *Future Anxiety*, representing anticipated anxiety about potential future threats; and (c) *Control Anxiety*, representing a user's sense of agency and perceived control over cybersecurity outcomes.

We used established methods for the development of CybAS (Fig. 1). We first reviewed the theories and research of cybersecurity, anxiety and privacy. Then, we conducted iterative survey studies and statistical analyses. Throughout, we held team discussions to reflect on findings and to examine the outputs for reliability and validity. The resulting instrument exhibits desirable psychometric properties of factor scoring, good Cronbach's alpha, and sufficient associations with related constructs. The number of items is short enough to be administered with other survey items. This enables HCI researchers to study the psychological dimensions of cybersecurity and offers practitioners a means to identify and address individuals experiencing heightened cybersecurity anxiety.

In summary, we contribute the following:

(1) *A diagnostic framework for understanding user-system breakdowns in cybersecurity***.** We introduce cybersecurity anxiety as a critical HCI construct that serves as an indicator of a misaligned mental model between a user and security technologies.
(2) *The development and validation of the Cybersecurity Anxiety Scale (CybAS)***,** a 15-item instrument that operationalizes this construct. We demonstrate how its three factors (Present, Future, Control) can be used to pinpoint specific user needs for improved interface design, training, and empowerment.
(3) *A vision for designing anxiety-reducing security interventions.* We present CybAS as a tool for the HCI community to design, implement, and evaluate new security systems—such as adaptive interfaces or targeted educational modules—that directly address the root causes of user anxiety.

2 RELATED WORK

In the following, we outline related work, explored during our extensive literature review. The goal of this review was to gain an overview of the domain surrounding cybersecurity anxiety and evaluate how the existing literature influences our work. Venues we visited throughout the literature review included two conferences, one for each of the two core topics "human computer interaction" (considered venue: CHI) and cybersecurity (considered venue: USENIX Security). In addition, other research and papers in the domains of clinical anxiety, privacy and cybersecurity were visited to include some different views. This allowed us to explore the standard methodology used for creating and concepts explored by those kind of scales.

2.1 Cybersecurity

Cybersecurity is a central concept for CybAS, but its definition varies across different domains. The term itself is not always self-explanatory and has gotten multiple interpretations depending on the context [6]. The focus can range from governmental protection of critical infrastructures to an individual's protection against malware and phishing attacks. Governmental definitions tend to focus on the protection of the institution. This means a focus on the infrastructure and operational up time, while the academic world frame cybersecurity more broadly by highlighting the complex interactions between technological infrastructures, organizational processes and human actors [20, 58]. Standardization bodies such as the National Institute of Standards and Technology (NIST) add an additional focus on cybersecurity protection goals, i.e., ensuring availability, integrity, authentication, confidentiality and non-repudiation [57]. These definitions show that cybersecurity can be interpreted in different ways covering both practical and conceptual aspects, with a focus on resilience, trust and protection against cybersecurity threats, regardless of whether they are accidental, intentional or natural.

Several psychometric scales have previously attempted to capture individuals' perceptions, attitudes or behaviors towards cybersecurity. An example of this is the Cybersecurity Scale (CS-S) [2], which measures practices and perceptions across six dimensions: availability, authenticity, confidentiality, integrity, possession/control and utility. While CS-S provides a valuable foundation for understanding how individuals approach cybersecurity, it does not address the potential emotional or anxiety related consequences of these practices.

The Human Cyber-Resilience Scale [45] instead focuses on attitudes, behaviors and resources that enable individuals or households to cope with cybersecurity incidents. It has a focus on self-efficacy, helplessness and social support, which makes it particularly relevant for CybAS when connecting cybersecurity behavior with emotional outcomes such as anxiety. Other related measures capture more specific aspects. The Cyber-Paranoia and Fear Scale [55] distinguishes between realistic and unrealistic fears, providing insight into how individuals perceive cybersecurity threats. The Security Attitude Scales (SA-6 and SA-13) [27, 29] measure users' attitudes toward cybersecurity measures. SA-6 assesses general engagement and attentiveness to security practices, while SA-13 extends this by adding dimensions of resistance and concernedness

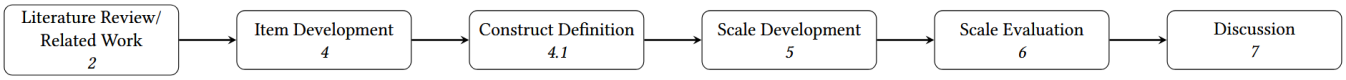

Figure 1: Structure of the Paper.

toward compliance. Behavioral intentions are instead addressed by the Security Behavior Intention Scale (SeBIS) [25], which covers password management, software updates, device securement and proactive awareness.

Although these scales offer valuable insight into cybersecurity practices, resilience, fear and behavior, none of them directly measure anxiety as a construct in relation to cybersecurity. Recognizing this gap motivated the development of CybAS as a way to capture cybersecurity related anxiety more directly.

2.2 Anxiety

Anxiety is defined as *an uncomfortable feeling of nervousness or worry about something that is happening or might happen in the future*[1]. Occasionally, it is normal to experience the feeling of anxiety in situations e.g., exams at school, finances or family problems [60]. However, anxiety can occur in different levels of severity. At a high severity, anxiety is unhealthy and is advised to be treated professionally. As the definition indicates, a huge number of different kinds of anxiety exist. Psychometric anxiety scales try to identify the severity of anxiety present in a individual.

Anxiety scales can be divided into two different spectrums. The first kind assesses anxiety in a clinical context [7, 33, 70, 80], which include the likes of the general anxiety disorder or social anxiety disorder [61]. Here, items often target either somatic or mental symptoms of anxiety [33, 70]. We especially deemed mental symptoms as crucial for assessing cybersecurity anxiety, including the likes of worry, fearful anticipation and anticipation of the worst. A challenge often occurring during development of an clinical anxiety scale is, whether the scale overlaps with the depression domain [70]. Even though the domains of anxiety and depression are related [70, 80], it is important to ensure that different constructs are measured, preventing that the presence of depression elevates the measured anxiety [22]. We saw clinical anxiety as crucial for understanding how anxiety is assessed, especially for examining which feelings are caused by anxiety.

The second kind of anxiety scales assess anxiety towards a specific domain [38, 44, 63, 66], including the likes of tests or examinations, health and artificial intelligence. Most of the domain-specific anxiety scales were closer to the construct of cybersecurity anxiety compared to the clinical anxiety scales. This led us to consider especially their content for the definition of cybersecurity anxiety and during the item generation (cf. Section 4.2). We identified the Computer Anxiety Rating Scale (CARS) [38] and the Artificial Intelligence Anxiety Scale (AIAS) [78] as central here, due to the close connection of both computers and artificial intelligence (AI) to cybersecurity.

We examined both clinical anxiety scales and domain-specific anxiety scales during development of CybAS. We saw clinical anxiety as relevant to inform development and test against CybAS, due to getting an understanding on how anxiety is assessed in general. However, domain-specific scales, especially concerning scales of which the domain is closely related to cybersecurity such as computers and AI, were seen as more relevant and closer to CybAS as a construct measure. We tested correlation towards both categories in the scale development process.

2.3 Privacy

Privacy describes *the state of being alone, or the right to keep one's personal matters and relationships secret*[2]. Here we especially saw the second part of the definition as crucial in regards to cybersecurity. Through the use of the internet, smartphones, and social media, society exposes much personal information, which is stored [52]. This makes it possible to monitor people, and misuse the available data. Besides this, data stored online is vulnerable to possible data breaches or cyberattacks [48]. These violate privacy and are closely related to the rapid development and spread of digital technologies in everyday life, which also increases the "attack surface" for potential breaches.

In this research we especially looked at three different facets of privacy: an individual's own privacy, information privacy [53] and other people's privacy [34]. For people's own privacy, we looked at their privacy concerns, which are shown to have influence on cybersecurity behavior [26]. People are especially concerned about identity fraud, lack of control and data misuse [56]. Information privacy focuses on the extend to which individuals think it is fair that their information is communicated to others [53]. We especially focused on how companies treat data, including selling information. Lastly, we saw other people's privacy [34] as important, because a theory known as the privacy paradox. The privacy paradox says that individuals concerns about privacy sometimes does not reflect the privacy management choices they make [5]. We examined the privacy of others with the idea that individuals might respond more honestly when considering others' privacy rather than their own.

Due to the strong relationship between cybersecurity and privacy, an online privacy violation is often also an cybersecurity violation, we saw privacy together with anxiety and cybersecurity as central aspects during development of CybAS. The finalized scale includes items that indicate this strong relationship.

2.4 Other Concepts

Besides the previously mentioned three main concepts, we examined other literature, which we were not able to classify under those concepts. These were for instance resources about affinity for

[1]Cambridge University Press. (Accessed on 26.02.2025). Anxiety. In Cambridge Dictionary. Retrieved from https://web.archive.org/web/20250226101448/https://dictionary.cambridge.org/dictionary/english/anxiety

[2]Cambridge University Press. (Accessed on 20.02.2025). Privacy. In Cambridge Dictionary. Retrieved from https://web.archive.org/web/20250220092608/https://dictionary.cambridge.org/dictionary/english/privacy

technology interaction [31], social media usage [62, 69] and social support [1, 9, 81]. We deemed affinity for technology interaction as relevant for the development of CybAS, through the hypothesis that people with higher affinity for technology interaction have higher chance of implementing better cybersecurity practices. Research has shown that strong attitudes, knowledge and confidence can lead to improved cybersecurity behavior [4, 27]. Social media usage was included by us to get a glimpse of individuals' online activities and how much data individuals expose on the net. We included this, because increased amount of personal data online, yields higher risk of becoming a victim of cyberattacks [54]. We did also see helplessness as a relevant concept for assessing cybersecurity anxiety. It was recognized both in the form of being helpless when an cyberattack occurs [3], but also helplessness or resignation arising when private data is provided to companies in exchange for a service [23, 68]. This tradeoff can lead to a sense of helplessness or a perceived lack of control over the management of personal data. Lastly, we examined social support to cover the factor which family friends and experts have in the case of a cyberattack. Multiple studies see a clear relation between social support and mental health [17, 19, 74], which we saw as crucial when assessing cybersecurity anxiety.

One of the main questions in developing CybAS was whether individuals with greater cybersecurity knowledge and more implemented protective measures would report lower or higher levels of cybersecurity anxiety. Both outcomes can be justified: higher anxiety may lead to more security measures taken, whereas greater security might reduce anxiety. This was closely monitored throughout the development of CybAS.

3 SCALE DEVELOPMENT PROCESS

We performed the scale development process following the recommendations of the literature on psychometric scale development [8, 18, 50]. The process was divided into three separate phases: the item development phase, the scale development phase and the scale evaluation phase. Each of the phases comprises several steps, as outlined below. We describe each of the phases in detail in subsequent sections.

Item Development (Section 4).

Step 1a *Conceptualization and domain identification:* Define cybersecurity anxiety based on literature and theoretical background.

Step 1b *Item generation:* The item generation process for creation of the initial item pool.

Step 1c *Assessing content validity:* Verification that the items measure the construct they claim to measure, cybersecurity anxiety.

Scale Development (Section 5).

Step 2a *Pilot survey:* Item reduction through a first screening.

Step 2b *Identification of factor structure:* Identification of the latent factors of the scale through appropriate analysis techniques.

Step 2c *Finalizing scale items:* Identification of best performing items, to be included into the final item set.

Scale Evaluation (Section 6).

Step 3a *Confirming the factor structure:* Analysis for the quality of the factor structure.

Step 3b *Test of reliability:* Evaluate whether the scale yields stable results, by assessing the scales internal consistency.

Step 3c *Test of validity:* Evaluate whether the scale measures what it claims to measure, by assessing correlation towards already validated scales in the domain.

4 ITEM DEVELOPMENT

The goal of the item development phase is to create a large sample of items, measuring the construct of cybersecurity anxiety. Each item created is rated on a 5-point Likert-type agreement scale (1=Strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly agree). We chose a 5-point Likert scale because of the appeal of the neutral element, which gives gives the participant a safe answer when an they are unsure on how they feel about an item. From this large sample the final items will be chosen throughout the process, facilitated by analysis. Besides this, we created a working definition for the construct of cybersecurity anxiety and assessed the generated items for content validity in this phase.

4.1 Conceptualization and Domain Identification

The first step in psychometric scale development is to define the construct [8, 18, 50]. This is done in order to have clarity on the scope we want to target with the scale. Due to the cybersecurity anxiety construct being rather unexplored, we wanted to target as much of the domain as possible. The construct was explored through an extensive literature review, which included examining existing research papers, validated scales and concerns related to the construct of cybersecurity anxiety. Some of the literature and concepts examined are mentioned in Section 2. Based on the literature review, we created the following working definition for the cybersecurity anxiety construct:

> Definition (Cybersecurity Anxiety). *Cybersecurity anxiety is described by two main aspects. Firstly, the feeling of discomfort, worry and nervousness (apprehension, fear, tension) stemming from potential cyberattacks performed by illegal/criminal/unauthorized third parties. Secondly, the feeling of helplessness and potential inability to deal with incoming cyberattacks. This feeling can be influenced by mental health conditions like depression and fear. Other factors such as a person's digital footprint, technological literacy and personal beliefs can lead to heightened levels of cybersecurity anxiety.*

Even though the definition tries to capture a broad scope of the cybersecurity anxiety domain, some concepts seen as relevant were not included in the definition, due to it failing to achieve the goal of a compact definition. These concepts include social support, self-efficacy, possible loss, risk perception, technology resilience and technology interest. To capture all these concepts, we created a nomological network (see Appendix C). The network gave us

the opportunity to illustrate possible interrelationships between constructs and connect observable manifestations to them.

4.2 Item Generation

With the domain defined, the next step was to create a large initial item pool, which we later used as a starting point for the scale development. The first step was to take inspiration from other sources examined in the literature review. This included items from existing scales without any adjustment, adapted items to better match the domain of cybersecurity anxiety, or newly generated items from concepts discussed in an examined research papers. Next, we generated items ourselves about concepts not discussed in the examined literature, but we deemed important for capturing the entire domain of cybersecurity anxiety. Here, we used the nomological network to ensure that the created items captured all concepts we deemed possibly relevant. To incorporate perspectives beyond the professional research area, we examined internet forums like Reddit [3] and Quora [4], to understand the fear and concerns of the broader public regarding cybersecurity. The examination of the forums lead us to generating items about artificial intelligence, helplessness, spying, excessive stress and additional privacy concerns.

The item generation phase consisted of six iterations. In each iteration, we examined new sources and visited new forums, to ensure full coverage of the subject domain. Furthermore, we reworded items to improve their clarity (so they would be easier to understand) and to elicit an increased variance among responses (to force a wider range of answers from the participants). Lastly, we also removed items which were very similar in wording to others. In total, 204 items were generated in the item generation phase.

4.3 Assessing Content Validity

To ensure that the generated items adequately capture the intended domain, we assess their content validity [8, 18, 39]. We used the nomological network to keep track of all concepts considered relevant to the domain, and to capture the entire domain in the item generation phase. During the item generation phase, the created items were continuously discussed inside the research team and, based on these discussions, refined to better capture the domain of cybersecurity anxiety.

To capture additional opinions on the generated items, we performed cognitive interviews with six people in the target population, i.e., technology users who were not involved in the research. These people were people related or friends of the research team and volunteered to help. They varied in age and amount of time they spent online, to get diverse impressions. The cognitive interviews were performed with the intention to get initial perceptions on the concepts and the generated items, both with regards to understandability and content. They were performed as one-on-one interviews in person or on a call. We would prompt them with one of the items and the participant would explain how they understood the respective item, whether they thought the item was relevant and whether any clarifications were needed. Lastly they were asked if they felt like any relevant items were missing. After the interviews, the wording and clarity of items were improved and prepared for the pilot survey, where further insight on the construct was gained. In the pilot survey it was possible for participants to leave feedback, which was used to further improve the clarity of items.

[3]Searched in Subreddit Anxiety, among others for the keywords: Cybersecurity, Artificial Intelligence and Hacked.

[4]Quora discussions regarding Cybersecurity and Getting Hacked. Found through searches on Cybersecurity, Anxiety and Hacked.

5 SCALE DEVELOPMENT

5.1 Participant Recruitment

We conducted three rounds of data collection to iteratively develop and validate CybAS (see Appendix D for full survey). All participants were recruited through Prolific, a crowdsourcing platform for academic research that was found to be in particular suitable for security and privacy work [72]. The survey was developed in SurveyXact. Eligibility criteria were consistent across the rounds, involving U.S. residents aged 18 or older, with a balanced gender split and an even distribution across the U.S. political spectrum. Participants were allowed to participate only once. Those who had completed an earlier round were excluded from all later survey rounds. Participants were compensated between $4.06 (£3.00) and $6.09 (£4.50) depending on the survey length. All human subjects research and data collection was reviewed and approved by authorities at the lead authors' institution.

The first round, our pilot, included $N = 301$ participants. The second round, aimed at identifying the factors structure, involved $N = 310$ participants. The third and final round focused on validation of the factor structure using a 28-item set with N = 275 participants. We describe all three rounds in detail in the remainder of this section. All analyses were based on complete and valid responses. We excluded participants if they failed attention checks, had missing responses, or selected the same answer possibility throughout the entire survey. See Table 1 for demographics of the three rounds.

5.2 Round 1 – Pilot

The initial CybAS item pool consisted of 204 items. To minimize respondent fatigue, the items were randomly split into four distinct sets ($Q_1 - Q_4$) and distributed in separate survey rounds [43]. Each respondent only saw one set, with the item order being randomized in order to mitigate ordering effects [64]. The pilot survey aimed to identify low performing items, primarily by focusing on low variance in item response distributions before conducting exploratory analyses.

We first calculated item response variances, which were calculated using the numerical responses to each Likert-type item and applied a cutoff threshold of > 1.1, resulting in the removal of 87 items. Then we performed an exploratory factor analysis (EFA) separately on the remaining items in $Q_1 - Q_4$. Items with low factor loadings ($< .40$) or cross-loadings ($> .40$) were discarded [71]. Additionally, we removed some full factors from Q_2 and Q_3 due to redundancy with constructs from established scales (e.g., SeBIS [25], SNAS [69]), leaving 63 items for further analysis.

5.3 Round 2 – Identification of Factor Structure

In the second round of data collection, we aimed to identify the factor structure of the refined 63-item set pool (see Appendix D). This survey was completed by N = 310 participants. We performed

	Round 1	*Round 2*	*Round 3*
N	301	310	275
Age			
18 – 24	7.9%	9.8%	7.9%
25 – 34	32.7%	26.9%	31.4%
35 – 44	29.7%	25.6%	20.7%
45 – 54	17.9%	20.4%	20.7%
55 – 64	5.9%	11.9%	12.9%
65 or older	5.9%	5.4%	6.4%
Gender			
Male	49.2%	50.0%	49.6%
Female	50.8%	50.0%	49.6%
Non-binary	0.0%	0.0%	0.8%
Ethnicity Simplified			
White	77.9%	66.6%	63.6%
Black	11.5%	24.7%	20.7%
Asian	3.0%	3.4%	4.3%
Mixed	4.6%	2.8%	7.9%
Other	3.0%	2.5%	3.2%
Prefer not to say	0.0	0.0%	0.3%
Political Status			
Liberal	36.5%	42.8%	37.5%
Conservative	29.2%	32.5%	33.6%
Moderate	29.6%	22.8%	26.1%
Other	4.7%	1.9%	2.8%
Level of Education			
Some High School or less	0.3%	0.3%	0.3%
High School Diploma or GED	13.6%	7.2%	9.1%
Some college, no degree	21.6%	10.6%	14.2%
Associates or technical degree	10.3%	5.3%	8.7%
Bachelors degree	32.6%	41.6%	37.5%
Graduate or professional degree	21.6%	35.0%	30.2%
Yearly Income			
Less than $31,200	15.3%	14.7%	13.1%
$31,201 – $49,999	16.9%	13.8%	14.5%
$50,000 – $74,999	17.3%	18.4%	18.2%
$75,000 – $99,999	16.9%	15.0%	15.6%
$100,000 – $149,999	18.6%	25.9%	23.6%
$150,000 or more	14.0%	11.6%	14.2%
Prefer not to say	1.0%	0.6%	0.5%
Employment Status			
Full-Time	48.2%	60.0%	54.3%
Part-Time	22.1%	20.6%	21.1%
Not in paid work	10.9%	7.8%	7.5%
Unemployed	9.6%	5.3%	7.9%
Data Expired	5.3%	3.8%	4.6%
Other	3.9%	2.5%	4.6%

Table 1: Demographic characteristics of participants.

an EFA using oblique rotation and the minimum residual extraction method. Three factors were extracted based on the scree plot and parallel analysis [36, 51, 79]. Items were retained if they had a factor loading > .40 on a single factor and did not cross-load. The EFA process reduced the item pool to 39 (see Appendix D). To further refine the scale, we conducted a manual content review to remove semantically redundant items. For instance, we retained the item "I regularly perform backups", while removing the semantically similar item "I make sure to backup my devices", based on a higher factor loading for the former. As a result of this refinement, the item pool was narrowed to 29. A final EFA confirmed a stable three factor solution for these 29 items:

(1) **Present.** The *Present* factor captures fears and concerns related to immediate or on-going cybersecurity threats that could occur in the present moment. Items in this factor covered common concerns such as being impersonated, tracked or hacked, as well as fears of losing personal data or experiencing breaches of online privacy.
(2) **Future.** The *Future* factor reflected concerns about anticipated or potential cybersecurity risks emerging from technological change. Items included fear of the internet, unease about the rapid advancement of technology, and a broader sense of unease about the future digital environment.
(3) **Control.** The *Control* factor represented proactive and preventive measures taken to mitigate cybersecurity risks. Items in this factor reflected actions and attitudes such as regularly performing backups, staying informed about cybersecurity practices and learning from the experiences of others who have dealt with cyberattacks.

Although both the *Present* and *Future* factors reflect cybersecurity fears and concerns, the main difference is that *Present* captures concrete, immediate concerns related to personal cybersecurity threats, that have an actionable reaction. In contrast, *Future* reflects more abstract and generalized anxiety about the digital future, including concerns that may seem infeasible to address.

Internal consistency was strong across all three factors with Cronbach's alpha of $\alpha_{Present} = .94$, $\alpha_{Future} = .80$ and $\alpha_{Control} = .76$, all above the recommended threshold of > .70 [73]. One additional item was removed due to a low factor loading, resulting in a 28-item scale for the subsequent finalization round.

5.4 Round 3 – Finalizing Scale Items

After the initial exploratory analyses, another survey was conducted with N = 275 participants, satisfying the recommended 10:1 responses-to-item ratio, which is commonly used for robust psychometric evaluation [40, 79]. This survey included the preliminary 28-item CybAS, presented alongside seven established and related psychometric scales to assess convergent validity.

We decided to include the following scales: the Security Behavior Intentions Scale (SeBIS) [25], the Affinity for Technology Interaction Scale (ATI) [31], the Human Cyber-Resilience Scale [45], the Security Attitude 6-item Scale (SA-6) [29], the Generalized Anxiety Disorder 7-item Scale (GAD-7) [70], the Computer Anxiety Rating Scale (CARS) [38] and the Cyber-Paranoia and Fear Scale [55]. These seven scales were selected to capture a broad range of constructs hypothesized as being related to cybersecurity anxiety, in order to get a good assessment of convergent validity [18]. SeBIS and SA-6 measure security related behaviors and attitudes respectively, offering insight into the connections between individuals' actions and their mindset in cybersecurity. The Human Cyber-Resilience Scale assesses coping and recovery following a cybersecurity incident, while the Cyber-Paranoia and Fear scale distinguishes between realistic and unrealistic threat perceptions, which could be helpful for

Factor	#	Item
Present:	1	I constantly worry about cybersecurity.
	2	I fear being impersonated online.
	3	I worry about people editing my social media page without my consent.
	4	I constantly worry about being tracked.
	5	I constantly fear losing my online data.
	6	I fear unauthorized access to my social media accounts.
	7	I often fear hackers reading old chat messages of mine.
Future:	8	I often worry about the rapid development in technology.
	9	I increasingly fear the internet.
	10	I believe artificial intelligence will become dangerous in the future.
	11	I feel like artificial intelligence makes my education useless.
Control:	12	I regularly review my account login history for unusual activity.
	13	I am up to date with the newest cybersecurity practices.
	14	I regularly perform backups.
	15	I am familiar with how someone I know has dealt with a cyberattack and intend to follow their example.

Table 2: Overview of the final CybAS items validated in the third survey round. We recommend to use a bidirectional Likert agreement scale for the item responses (e.g., 1=Strongly Disagree to 5=Strongly Agree) and average the ratings to compute the factor scores and overall CybAS score. See Section A for the instructions that our survey gave to participants and Section 6.4 for suggested benchmarks.

understanding the nature of cybersecurity anxiety. GAD-7 provides a benchmark for general anxiety symptoms and can help explore whether cybersecurity anxiety represents a domain specific form of anxiety. CARS measures technology specific anxiety, allowing for a comparison between general technology apprehension and cybersecurity anxiety. Lastly, the ATI scale captures the differences in how individuals engage with technology, which may influence their risk assessment and responses to cybersecurity threats.

To further refine CybAS, we assessed the internal consistency of each factor using Cronbach's alpha and conducted a confirmatory factor analysis (CFA) [10, 11, 47] to evaluate the construct validity. Although the 28-item CybAS had strong internal consistency across factors, the CFA fit indices indicated only a marginal fit (CFI=.839, TLI=.824, RMSEA=.083, SRMR=.077) [10, 42, 47]. To improve model fit, we applied item response theory (IRT) to evaluate item performance [18, 24, 30] . Items were considered for removal based on empirical evidence, specifically those exhibiting relatively low item-total correlations (from Cronbach's alpha) and a weak IRT discrimination parameter compared to other items within their respective factors. This data driven approach ensured that scale reliability and validity were improved without compromising the conceptual integrity of the construct. One exception was made for the item "I believe artificial intelligence will become dangerous in the future," which was retained despite its comparatively lower statistical performance, as it had the highest factor loading in previous analyses and was deemed conceptually important for capturing the full scope of the construct. Following this process, 13 items were removed, resulting in a concise 15-item CybAS scale (Table 2).

6 SCALE EVALUATION

In the following we present the factor structure confirmation and the tests for reliability and validity on the final 15-item version of CybAS, indicating that it is a sound psychometric scale.

6.1 Confirming the Factor Structure

Earlier we identified a three factor structure for CybAS, using EFA. We confirmed this structure using confirmatory factor analysis (CFA) [10, 11, 47]. The CFA was run using the lavaan package in R, and the model converged after 40 iterations. The maximum likelihood (ML) estimator with non-linear minimization with bounds (NLMINB) optimization was used and the following goodness of fit indices were examined: the Root Mean Square Error of Approximation (RMSEA), the Standardized Root Mean Square Residual (SRMR), the Comparative Fit Index (CFI) and the Tucker-Lewis Index (TLI). The analysis identified for the incremental fit indices the values RMSEA = .071 and SRMR = .06, which is within acceptable thresholds, which are .08 (RMSEA) and .06 (SRMR) respectively [10, 42]. For the absolute fit indices, values of CFI = .942 and TLI = .930 were identified, which also are in the range of acceptable model fit above .90 [10, 47]. See Appendix B for the standardized estimates and standardized correlations among the latent factors for the finalized CybAS.

6.2 Test of Reliability

Reliability is assessed to confirm that the scale results are consistent [8, 59]. We looked at the Cronbach's alpha [73] values to assess the reliability. Because the alpha only can be used for unidimensional scales, the alpha was calculated for each of the three factors separately. A Cronbach's alpha of $\alpha_{Present}$ = .92, α_{Future} = .77, and $\alpha_{Control}$ = .76 shows high internal consistency for CybAS,

Scale	Full CybAS	Present	Future	Control
Security Attitude 6 item (SA6)	$r = .616,\ p = 0$	$r = .561,\ p = 0$	$r = .139,\ p = .021$	$r = .772,\ p = 0$
Cyber Paranoia and Fear Scale	$r = .505,\ p = 0$	$r = .484,\ p = 0$	$r = .537,\ p = 0$	$r = .139,\ p = .021$
Affinity for Technology Interaction (ATI)	$r = .350,\ p = 0$	$r = .342,\ p = 0$	$r = -.036,\ p = .549$, n.s.	$r = .509,\ p = 0$
Security Behavior Intention Scale (SeBIS)	$r = .257,\ p = 0$	$r = .194,\ p = .001$	$r = .002,\ p = .974$, n.s.	$r = .465,\ p = 0$
Computer Anxiety Rating Scale (CARS)	$r = .221,\ p = 2e-04$	$r = .164,\ p = .007$	$r = .433,\ p = 0$	$r = -.044,\ p = .472$, n.s.
Human Cyber Resilience	$r = .206,\ p = 6e-04$	$r = .194,\ p = .001$	$r = -.173,\ p = .004$	$r = .473,\ p = 0$
General Anxiety Disorder 7 item (GAD7)	$r = .106,\ p = .081$, n.s.	$r = .094,\ p = .119$, n.s.	$r = .250,\ p = 0$	$r = -.100,\ p = .099$, n.s.

Table 3: Pearson correlation coefficients between CybAS full scale and subscales with external measures. n.s. indicates non significant results (p > .05).

above the required threshold of > .70 [73]. In addition, we calculated the reliability for the full 15-item scale, treating it as a unidimensional scale. This assesses its potential use as a single, holistic measure of cybersecurity anxiety. The full-scale Cronbach's alpha was $\alpha_{Full} = .90$, indicating strong internal consistency across all items.

To complement Cronbach's alpha, and provide a more theoretically robust estimate, we also computed McDonald's omega. Omega provides a more accurate estimate of reliability when the assumption of tau-equivalence is violated, which occurs when items have unequal factor loadings, as is common in multidimensional scales [35]. This makes omega particularly suitable for the three-factor structure of CybAS. The resulting omegas per factor were $\omega_{Present} = .92$, $\omega_{Future} = .76$, and $\omega_{Control} = .76$, closely matching the Cronbach's alphas and confirming that each factor is internally consistent.

6.3 Test of Validity

Validation of a scale is tested to see whether a scale measures what it claims to be measuring [8, 18]. We assessed content validity (Section 4.3), and continue with construct validity. Construct validity was assessed through convergent validity, by calculating the Pearson correlation coefficient [18, 32] towards already validated scales related to the domain of cybersecurity anxiety. For this purpose, the scales we wanted to calculate correlation towards were included into the survey alongside CybAS. Each scale included had their own separate page in the survey and the order of questions was randomized. Additionally, we attempted to obtain the original instructions for the scales whenever possible. Among others, scales concerning clinical anxiety and scales concerning attitude, fear and intention towards security behaviors were included. The full list of included scales together with the Pearson correlation towards CybAS can be seen in Table 3.

From the results it can be seen that CybAS has significant positive correlations with related cybersecurity constructs such as the Cyber-Paranoia and Fear Scale [55] and SeBIS [25]. Conversely, we could identify no significant correlation between CybAS and the clinical anxiety scales GAD-7[70]. This matches our assumption that cybersecurity anxiety could be more of a domain specific anxiety. Taking a closer look at the CybAS subscales, each dimension shows a distinct pattern of associations with the external measures. The Present subscale, reflecting immediate cybersecurity worries, shows the strongest correlations with the Security Attitude and Cyber-Paranoia and Fear scales. The Future subscale, representing anticipatory concerns, shows the strongest correlation with Cyber-Paranoia and moderate correlations with technology anxiety, while associations with behavioral scales are generally weaker. The Control subscale, reflecting perceived lack of control over cybersecurity outcomes, shows the strongest correlation with Security Attitude and moderate correlations with technology engagement, resilience, and behavioral intention scales.

6.4 Benchmarks for Average CybAS Scores

From the results it was shown that the mean of participants' average CybAS test scores (items 1-15, Table 2) was 3.09 and the standard deviation intervals were $\pm1\sigma$ = [2.27, 3.9], $\pm2\sigma$ = [1.46, 4.71]. This can be used to give an estimate of an individual's level of cybersecurity anxiety compared to an average score for our U.S. population sample. The intervals from our collected data are:

- < 2.27 = Less than the average score for our U.S. population sample.
- 2.27 to 3.9 = Close to the average score for our U.S. population sample.
- > 3.9 = Higher than the average score for our U.S. population sample.

It is important to mention that these intervals are specific to our collected data sample and could look different for other data samples. Because of this it is always advised to calculate the intervals again when collecting new data. The mean scores and standard deviation of the subscales were also recorded to have a reference value when only assessing one of the subscales. For the *Present* factor a mean of 3.16 was recorded ($\pm1\sigma$ = [2.08, 4.24], $\pm2\sigma$ = [1.0, 5.31]), while the *Future* factor showed a mean of 2.73 ($\pm1\sigma$ = [1.8, 3.67], $\pm2\sigma$ =

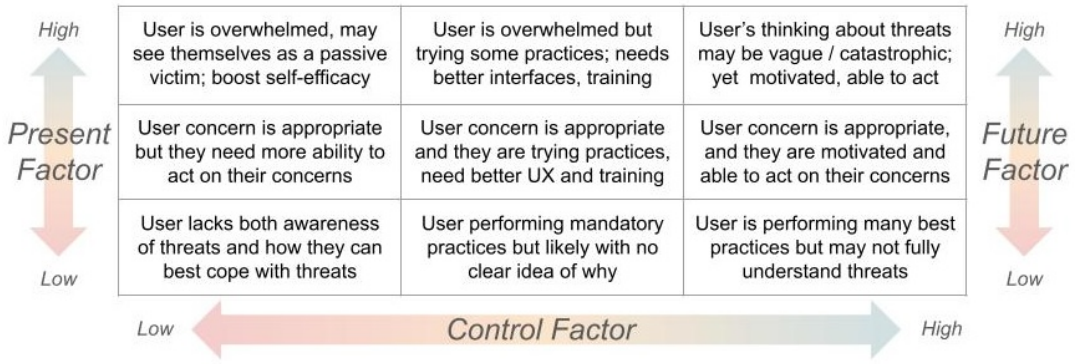

Figure 2: Hypothesized diagnostic categories based on CybAS subscale score combinations. The vertical (y) axes categorize users by their levels (Low or High) of both Present Anxiety and Future Anxiety, while the horizontal (x) axis indicates the level of Control Anxiety (Low or High). Each cell identifies a specific potential hypothesized user state and potential intervention needs (e.g., improved UX or training) for that profile. Whether users would actually be in these hypothesized states — given their ratings on the respective factors — is an important line of future work.

[0.87, 4.6]). Lastly, for the *Control* factor a mean of 3.31 ($\pm1\sigma$ = [2.42, 4.21], $\pm2\sigma$ = [1.52, 5.1]) was recorded.

7 DISCUSSION

This study developed and validated a self-report psychometric scale in order to measure cybersecurity anxiety. It resulted in the creation of the Cybersecurity Anxiety Scale (CybAS), a self-report 5-point Likert scale consisting of 15 items. Its development followed a standard process for psychometric scale creation [8, 18, 50]. To that end, we first defined the construct of cybersecurity anxiety and then refined CybAS through a multi-stage process encompassing item development, scale development, and scale evaluation. The final 15-item CybAS scale demonstrated a stable three factor structure, showing desirable psychometric properties in regards to reliability and validity. The following discussion places these findings within the context HCI research, emphasizing their implications for understanding user anxiety and establishes a starting point for anxiety-aware design.

7.1 A Diagnostic Tool for Understanding the User's Inner World

This study's primary contribution is not just the creation of a new scale, but the delivery of a valuable diagnostic tool for the HCI community. The 15-item Cybersecurity Anxiety Scale (CybAS) allows us to contextualize observed user behaviors by understanding the emotions tied to the underlying mental models that produce them.

7.1.1 How to Use the Overall CybAS Score. We believe that our factor structure and strong results for validity and reliability indicate that it is appropriate to compute and use an overall CybAS score from the average of the three scales. Further, the significant positive inter-correlations of all three factors (c.f. Section 6.1, Appendix B) tells us that it would not be appropriate to reverse-score one factor. Instead, we think the data is telling us that as cybersecurity anxiety rises with more awareness of real-world and hypothetical threats, so perhaps does the impulse to control the anxiety by acting on cybersecurity recommendations. Our thinking also is informed by our reading of the anxiety and mental-models literature, notably the nuances of GAD-7 and relevant DSM-5 entries, e.g., [49], as well as the Security and Privacy Acceptance Framework (SPAF) [21, 28] and earlier human-centered work in mitigating cyberattacks, e.g. [41]. The latter posits that people need Awareness, Motivation, and Ability to accept and adopt best practices (SPAF) and that, even when these obstacles are removed, end users require good interfaces and training to participate effectively in cyber-defense. The former suggest that a moderate amount of anxiety can lead to appropriate caution, and that anxiety is especially maladaptive when it paralyzes people from taking control actions. We can foresee, for example, that a user becomes so afraid of a security breach that they fail to install updates or effectively use a password manager, thus increasing their risk.

7.1.2 How to Use the Individual CybAS Factor Scores. The scale's three-factor structure (Present, Future, and Control) provides a new lens for HCI researchers to deconstruct the complex emotional and cognitive state of a user navigating today's threat landscape. Thereby, we envision that each of CybAS's factors can serve different purposes (Fig. 2).

To support this interpretation, Figure 2 visualizes how different combinations of CybAS factor scores may co-occur. The horizontal dimension (x) represents perceived Control, ranging from low to high ability to act on cybersecurity concerns. The vertical dimension (y) reflects how individuals score on Present and Future anxiety, combined into one level to allow capturing whether concern is driven by immediate usability challenges, abstract future threats, or a balance of both. A suitable relationship for this combination of the two factors should be the subject of future research. By reading the figure as a matrix rather than a classification scheme, researchers can reason about how different anxiety profiles interact with perceived control and what types of interventions may be

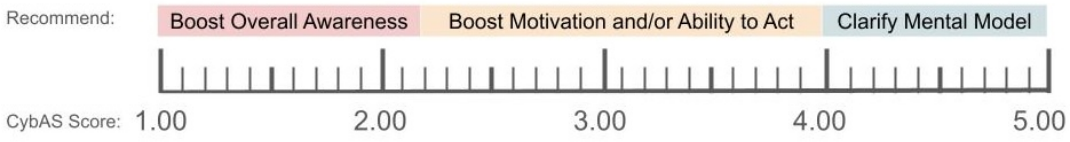

Figure 3: An overview of how to interpret the overall CybAS score, based in SPAF [21, 28]. The "sweet spot" for balancing different types of anxiety with control may lie in the middle values. Better interfaces and training may help boost their motivation and ability to act.

most appropriate. For instance, users reporting high Control alongside moderate levels of both Present and Future anxiety appear to represent a comparatively functional balance between concern and action, whereas other regions of the matrix suggest different mismatches between awareness, anxiety, and ability to respond.

Using this theoretical grounding for CybAS interpretation (Fig. 3), we hypothesize that a *moderate* overall CybAS score (in our sample, average 2.27 to 3.90 on a 5.00 scale) may be closest to the optimum for balancing different types of anxiety with control. Those individuals still may need better interfaces or training to help boost their motivation and ability to engage in recommended security practices. A *high* overall CybAS score (with high scores across Present, Future, and Control, average greater than 3.90/5.00) may indicate unreasonable anxiety that yet motivates useful actions to address real-world threats. Those individuals may need targeted training or feedback from systems, or both, to help clarify their mental models. Those with a *low* overall CybAS score (with low scores across all three factors, average less than 2.27/5.00) possibly have both very low awareness of cybersecurity threats and of how to cope with these threats. If these are true, then these end users need interventions to boost their general awareness of threats and to improve their security learning, which prior work indicates is a precursor to action [28].

For instance, when used in usability evaluations, high scores on the *Present* factor might indicate that a user is overwhelmed by the immediate usability challenges of the current security tasks, suggesting an ill-designed interface with insufficient affordances or a mental model cluttered with confusing or conflicting procedures (potentially even a combination of both). Thus, the factor might be used to identify a need for (a) improved interface designs and clearer system feedback, or (b) awareness measures that help address misconceptions or clutter stemming from misaligned mental models.

Similarly, high scores on the *Future* factor can indicate mental models dominated by vague, catastrophic threats learned from (social) media, suggesting a need for targeted training and educational interventions that build accurate threat models and debunk misinformation about cybersecurity threats.

Last but not least, a high perceived sense of control, indicated by a high score on the *Control* factor, might be a strong signal of a mental model in which the user has much to lose and want to protect their values as well as possible. With high knowledge on how to control against cybersecurity incidents, a good chance on high knowledge of what can follow from cybersecurity incidents. Even though perfect control measures are implemented, safety cannot be guaranteed also because personal data stored by companies are beyond personal agency. The Control factor might indicate the necessity for increased information sharing towards what can and what cannot be controlled regarding cybersecurity, as well as how to recover from a cybersecurity incident so that even though it is impossible to ensure full control, a clear path to recovery can be ensured.

Our analysis of the inter-factor correlations provides a critical insight. The weak link between *Future* anxiety (abstract threats) and *Control* (concrete actions) gives empirical weight to a long-standing HCI challenge: users may be aware of distant dangers but fail to translate that awareness into immediate protective behaviors. This signals a breakdown in their mental model, where the threat and the solution are disconnected. Similarly, the finding that taking more control actions can positively correlate with anxiety challenges the simplistic notion that "more security features" or "more user education" are inherently good, without considering the context. If our interventions increase a user's cognitive load without increasing their sense of self-efficacy, we may be inadvertently increasing their anxiety, leading to burnout and disengagement.

7.2 Cybersecurity Anxiety as a Design Problem

A key step in our validation was distinguishing cybersecurity anxiety from generalized clinical anxiety (GAD-7). This distinction is vital for HCI because it scopes the problem appropriately: cybersecurity anxiety is not an innate user pathology but a domain-specific, context-driven response to technology.

This reframes it as a design problem. We argue that cybersecurity anxiety must not be met with therapy, but instead represents the HCI challenge to come up with accommodating designs. The solution lies not in clinical intervention, but in building better, more humane systems. If a user is anxious about cybersecurity, we suggest that the root cause is likely found in confusing interfaces, opaque security processes, or a feeling of powerlessness instilled by the technology itself or constant data breaches.

Therefore, we believe that CybAS empowers designers and researchers by making the problem tractable. We can and should address this form of anxiety through improved interaction designs, system feedback, and targeted training. CybAS gives us a reliable way to measure whether our design interventions are working in increasing users' sense of control and decreasing their overall cybersecurity anxiety, regardless of whether directed at present or future issues.

7.3 A Vision for Anxiety-Aware Design

The development of CybAS opens up several new avenues for HCI research and practice, moving us from merely identifying cybersecurity anxiety to actively designing against it.

For HCI research, CybAS can now be used as a core metric in usability and security studies. Researchers can, for instance, conduct A/B tests of different security interfaces (e.g., a simplified vs. expert-level password manager) and use CybAS to measure which design leads to lower "Present" anxiety scores. Longitudinal studies can use the scale to track how users' mental models and anxiety levels evolve after interventions, such as immediately after phishing training or a data breach and then at three-, six-, and twelve-month marks afterward. Interventions that might be particularly suitable for this are phishing simulation campaigns performed as awareness measure in organizations which have been shown to induce stress and other negative emotions in affected employees [12].

For HCI practitioners, the insights from CybAS can directly inform the creation of anxiety-aware systems. For example, a system could use a user's CybAS profile to become adaptive, offering more guidance and reassurance to those with high anxiety scores. Designers also can focus on interventions that specifically target the Control factor. This might include creating security dashboards that clearly visualize a user's protection status, providing simple, actionable checklists, or designing 2FA prompts that explain why a step is necessary, thereby replacing uncertainty with understanding and empowerment. For instance, password security audit dashboards included in password managers have been found to overwhelm users [46] and their information being in turn ignored by them [15].

In essence, we provide a vision for research vision in HCI focused on the psychological and emotional dimensions of security. CybAS represents an essential enabling tool for that vision. It allows us to get a more nuanced impression of users' mental models and, most importantly, allows us as HCI community to build systems that not only protect users' data but also safeguard their peace of mind.

7.4 Limitations

CybAS is, among other things, limited by the demographics of the survey participants. Firstly, we only collected data from U.S. citizens during development of the scale. While there was an even split between men and women, and a roughly even distribution across the political spectrum, most of the participants where white, on the younger end and had a high level of education. Other regions, age groups, and ethnicities could have had different views and opinions on the topic. This could have led to different results in the scale creation, in terms of selected items and identified factors. Additionally, the scale has only been checked for reliability and validity within the corresponding demographics, indicating that major differences in views on cybersecurity might affect the validity of CybAS for other demographic groups. In addition, we also tried to perform an analysis of variance (ANOVA) [65] during the scale development process, to assess whether levels of cybersecurity anxiety differ across demographic groups. However, due to the imbalance of participants across demographic groups, it was not possible to identify any meaningful differences.

Furthermore, all data was collected through online surveys. Even though measures like attention checks were implemented to increase data quality, other delivery methods of our survey might have yielded different results. Similarly, we tried to minimize respondent fatigue by, e.g., limiting the length of the questionnaires, we cannot be one hundred percent sure that there is no bias or fatigue present.

Another potential limitation, is our broad definition of cybersecurity anxiety. The initial aim was to cover a wide range of concepts related to cybersecurity anxiety. This led to a large number of items, with a relatively even split between the different concepts. It is possible that some nuances were overlooked or only partially addressed during the scale development. Also, the *Present* factor has a larger number of items, compared to the remaining two factors, *Future* and *Control*. Even though the *Present* factor has the largest internal consistency and the highest factor loading, this could possibly lead to skewed results when assessing cybersecurity anxiety. Imagine two participants, from which one has a high score in the *Present* factor and the *Future* factor, while both having a score of zero in the remaining factor. The participant with the higher score in *Present* would have a higher score for cybersecurity anxiety as well, even though they not necessarily would be more anxious compared to the other participant. When comparing and evaluating scores the difference in factor size must therefore be kept in mind.

Finally, our hypotheses in Section 7.1 as to how to interpret CybAS scores are grounded in theory from prior work. While the scale and its factors have exhibited significant associations with each other and with other well-known scales, helping to guide our interpretations, future work will be needed to investigate how well CybAS performs as a diagnostic tool and whether our recommendations will need adjustment.

7.5 Future Work

To improve CybAS in future work, more balanced demographics and further geographic regions should be explored. With more demographics the analysis of variance could be revisited to possibly identify demographic groups which are especially anxious towards cybersecurity. Collecting data from further regions could make the scale more sound and increase the value for more people.

Additionally, CybAS has not been evaluated for its performance over time or as a diagnostic tool. The former could be addressed by assessing test-retest reliability or perform long-term longitudinal studies to examine changes in test scores over time. Performing this analysis would also increase the reliability of the CybAS scale. For the latter, rigorous empirical validation will be needed to confirm that specific score ranges accurately correspond to distinct behavioral outcomes and cognitive states in real-world settings. Future long-term studies can establish cut-off points shown to reliably distinguish between adaptive security caution and maladaptive, paralyzing anxiety.

During the development of the scale the *Control* factor was explored, which might indicate that higher levels of cybersecurity measures taken may be associated with higher levels of cybersecurity anxiety. It is difficult to draw definitive conclusions based on this research as this was not its main focus. However, it could be a

valuable direction of future work to further explore the implications between the two concepts.

CybAS was tested for correlation towards the seven scales seen in Table 3. From those a relatively even split between strong, moderate, lower and insignificant correlations can be seen. We chose these scales, because we thought there was a good chance for correlation between CybAS and the other included scales, with the exception of GAD-7. In order to prevent respondent fatigue and ensure high quality data, no further scales were included in the survey. Nonetheless, this does not preclude that other scales with strong correlation towards CybAS exist. In particular, it might prove worthwhile to test CybAS towards relevant privacy scales like the Value of Other Peoples Privacy [34], scales measuring more domain specific anxieties like the Artificial Intelligence Anxiety Scale [78] and other domains related to cybersecurity.

Due to the domain of cybersecurity anxiety being rather unexplored, CybAS can be taken as a starting point to further explore that domain. As outlined above, a valuable line of future work could be to develop interventions designed to address and decrease users' cybersecurity anxiety. Here CybAS could possibly be used to identify what people with increased or low levels of cybersecurity anxiety have in common, to identify what fears are present and explore what can be done to help and mitigate cybersecurity anxiety. After the development of intervention methods, CybAS could be used to assess changes in cybersecurity anxiety levels and evaluate the effectiveness of the interventions.

8 CONCLUSION

Emotions towards cybersecurity mechanisms have been recognized as central factor in influencing individual's cybersecurity behavior. Within this context, the construct of cybersecurity anxiety is a critical yet underexplored phenomenon. The cybersecurity anxiety scale (CybAS), a Likert-type scale comprising three factors (*Present*, *Future* and *Control*) offers a structured means of capturing different dimensions of cybersecurity anxiety. Analysis of CybAS demonstrated sufficient psychometrics properties regarding both reliability and validity. While further exploration on demographics should be performed, we suggest that the scale consistently assesses cybersecurity anxiety. Moreover, the absence of significant correlations with established clinical anxiety scales suggests that cybersecurity anxiety is a domain-specific construct, reflecting context-driven responses to technological environments rather than generalized clinical anxiety

CybAS represents an important foundation for research into cybersecurity anxiety. Future studies could use CybAS to investigate the underlying causes of cybersecurity anxiety and with the findings design more anxiety-aware systems. Given the relative novelty of the cybersecurity anxiety construct, ongoing research will be essential to refine our understanding and to develop practical strategies that mitigate its impact. Ultimately, advancing knowledge in this area has the potential to foster safer, more supportive interactions between individuals and digital technologies.

ACKNOWLEDGMENTS

This work was supported by the Digital Democracy Centre (DDC), University of Southern Denmark, through a DDC Thesis Grant. We thank the Centre for its support of research into the societal and psychological dimensions of digital technology and cybersecurity.

This work was also supported by the Topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by the KASTEL Security Research Labs. Faklaris was partially supported by U.S. National Science Foundation (NSF) Grant No. 2346281, DOD Department of the Army (DA) Grant No. W911NF2410189, Google, and BasisTech founder Carl Hoffman.

We also thank our CHI reviewers for their time and helpful feedback.

REFERENCES

[1] Gavin Andrews, Christopher Tennant, Daphne M Hewson, and George E Vaillant. 1978. Life event stress, social support, coping style, and risk of psychological impairment. *The Journal of nervous and mental disease* 166, 5 (1978), 307–316.
[2] Ibrahim Arpaci and Kadir Sevinc. 2022. Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development* 38, 2 (2022), 218–226.
[3] George Ashenmacher. 2016. Indignity: Redefining the Harm Caused by Data Breaches. 51 Wake Forest L. *Rev* 1 (2016).
[4] Dennik Baltuttis, Timm Teubner, and Marc TP Adam. 2024. A typology of cybersecurity behavior among knowledge workers. *Computers & Security* 140 (2024), 103741.
[5] Lemi Baruh, Ekin Secinti, and Zeynep Cemalcilar. 2017. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication* 67, 1 (2017), 26–53.
[6] Morten Bay. 2016. What is cybersecurity. *French Journal for Media Research* 6 (2016), 1–28.
[7] Aaron T Beck, Norman Epstein, Gary Brown, and Robert A Steer. 1988. An inventory for measuring clinical anxiety: psychometric properties. *Journal of consulting and clinical psychology* 56, 6 (1988), 893–897.
[8] Godfred O. Boateng, Torsten B. Neilands, Edward A. Frongillo, Hugo R. Melgar-Quiñonez, and Sera L. Young. 2018. Best Practices for Developing and Validating Scales for Health, Social, and Behavioral Research: A Primer. *Frontiers in Public Health* 6 (2018). https://doi.org/10.3389/fpubh.2018.00149
[9] Patricia A Brandt and Clarann Weinert. 1981. The PRQ—a social support measure. *Nursing research* 30, 5 (1981), 277–280.
[10] Timothy A Brown. 2015. *Confirmatory factor analysis for applied research*. Guilford publications.
[11] Timothy A Brown, Michael T Moore, et al. 2012. Confirmatory factor analysis. *Handbook of structural equation modeling* 361 (2012), 379.
[12] Lina Brunken, Annalina Buckmann, Jonas Hielscher, and M. Angela Sasse. 2023. "To Do This Properly, You Need More Resources": The Hidden Costs of Introducing Simulated Phishing Campaigns. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 4105–4122. https://www.usenix.org/conference/usenixsecurity23/presentation/brunken
[13] Sanja Budimir, Johnny RJ Fontaine, Nicole MA Huijts, Antal Haans, George Loukas, and Etienne B Roesch. 2021. Emotional reactions to cybersecurity breach situations: scenario-based survey study. *Journal of medical Internet research* 23, 5 (2021), e24879.
[14] AJ Burns, Tom L Roberts, Clay Posey, and Paul Benjamin Lowry. 2019. The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research* 30, 4 (2019), 1228–1247.
[15] Patricia Arias Cabarcos and Peter Mayer. 2025. 'The more accounts I use, the less I have to think': A Longitudinal Study on the Usability of Password Managers for Novice Users. In *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*. USENIX Association, Seattle, WA, 351–369. https://www.usenix.org/conference/soups2025/presentation/cabarcos
[16] L Jean Camp. 2004. Mental models of computer security. In *Financial Cryptography: 8th International Conference, FC 2004, Key West, FL, USA, February 9-12, 2004. Revised Papers 8*. Springer, 106–111.
[17] John Cassel. 1976. The contribution of the social environment to host resistance: the Fourth Wade Hampton Frost Lecture. *American journal of epidemiology* 104, 2 (1976), 107–123.
[18] K. Coaley. 2010. *An Introduction to Psychological Assessment and Psychometrics*. SAGE Publications.
[19] Sidney Cobb. 1976. Social support as a moderator of life stress. *Biopsychosocial Science and Medicine* 38, 5 (1976), 300–314.

[20] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. 2014. Defining cybersecurity. *Technology innovation management review* 4, 10 (2014).

[21] Sauvik Das, Cori Faklaris, Jason I. Hong, and Laura A. Dabbish. 2022. The Security & Privacy Acceptance Framework (SPAF). *Foundations and Trends® in Privacy and Security* 5, 1-2 (2022), 1–143. https://doi.org/10.1561/3300000026

[22] Margien E den Hollander-Gijsman, Klaas J Wardenaar, Edwin de Beurs, Nic JA van der Wee, Ab Mooijaart, Stef van Buuren, and Frans G Zitman. 2012. Distinguishing symptom dimensions of depression and anxiety: An integrative approach. *Journal of Affective Disorders* 136, 3 (2012), 693–701.

[23] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New media & society* 21, 8 (2019), 1824–1839.

[24] Maria Orlando Edelen and Bryce B Reeve. 2007. Applying item response theory (IRT) modeling to questionnaire development, evaluation, and refinement. *Quality of life research* 16 (2007), 5–18.

[25] Serge Egelman and Eyal Peer. 2015. Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*.

[26] Musaddag Elrayah and Saima Jamil. 2023. Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness. *International Journal of Cyber Criminology* 17, 2 (2023), 166–187.

[27] Cori Faklaris, Laura Dabbish, and Jason I Hong. 2022. Do They Accept or Resist Cybersecurity Measures? Development and Validation of the 13-Item Security Attitude Inventory (SA-13). *arXiv preprint arXiv:2204.03114* (2022).

[28] Cori Faklaris, Laura Dabbish, and Jason I. Hong. 2024. A Framework for Reasoning about Social Influences on Security and Privacy Adoption. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, Article 16, 13 pages. https://doi.org/10.1145/3613905.3651012

[29] Cori Faklaris, Laura A Dabbish, and Jason I Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*.

[30] M YANG Frances and T KAO Solon. 2014. Item response theory for measurement validity. *Shanghai archives of Psychiatry* 26, 3 (2014), 171.

[31] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467.

[32] Frederick J Gravetter and Larry B. Wallnau. 2015. *Statistics for the Behavioral Sciences 10th edition.* Cengage Learning.

[33] Max Hamilton. 1959. THE ASSESSMENT OF ANXIETY STATES BY RATING. *British Journal of Medical Psychology* 32 (1959), 50–55. Issue 1. https://doi.org/10.1111/j.2044-8341.1959.tb00467.x

[34] Rakibul Hasan, Rebecca Weil, Rudolf Siegel, and Katharina Krombholz. 2023. A psychometric scale to measure individuals' value of other people's privacy (VOPP). In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–14.

[35] Andrew F Hayes and Jacob J Coutts. 2020. Use omega rather than Cronbach's alpha for estimating reliability. But… *Communication Methods and Measures* 14, 1 (2020), 1–24.

[36] James C. Hayton, David G. Allen, and Vida Scarpello. 2004. Factor Retention Decisions in Exploratory Factor Analysis: a Tutorial on Parallel Analysis. *Organizational Research Methods* 7, 2 (2004), 191–205. https://doi.org/10.1177/1094428104263675

[37] Richard G Heimberg, KJ Horner, HR Juster, SA Safren, EJ Brown, FR Schneier, and MR Liebowitz. 1999. Psychometric properties of the Liebowitz social anxiety scale. *Psychological medicine* 29, 1 (1999), 199–212.

[38] Robert K Heinssen Jr, Carol R Glass, and Luanne A Knight. 1987. Assessing computer anxiety: Development and validation of the computer anxiety rating scale. *Computers in human behavior* 3, 1 (1987), 49–59.

[39] Timothy R Hinkin. 1995. A review of scale development practices in the study of organizations. *Journal of management* 21, 5 (1995), 967–988.

[40] Timothy R Hinkin, J Bruce Tracey, and Cathy A Enz. 1997. Scale construction: Developing reliable and valid measurement instruments. *Journal of Hospitality & Tourism Research* 21, 1 (1997), 100–120.

[41] Jason Hong. 2012. The state of phishing attacks. *Commun. ACM* 55, 1 (Jan. 2012), 74–81. https://doi.org/10.1145/2063176.2063197

[42] Li-tze Hu and Peter M Bentler. 1999. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal* 6, 1 (1999), 1–55.

[43] Dahyeon Jeong, Shilpa Aggarwal, Jonathan Robinson, Naresh Kumar, Alan Spearot, and David Sungho Park. 2023. Exhaustive or exhausting? Evidence on respondent fatigue in long surveys. *Journal of Development Economics* 161 (2023), 102992.

[44] Deborah G Johnson and Mario Verdicchio. 2017. AI anxiety. *Journal of the Association for Information Science and Technology* 68, 9 (2017), 2267–2270.

[45] Adam N Joinson, Matt Dixon, Lynne Coventry, and Pam Briggs. 2023. Development of a new 'human cyber-resilience scale'. *Journal of Cybersecurity* 9, 1 (2023).

[46] Emiram Kablo, Katharina Kader, and Patricia Arias-Cabarcos. 2024. "I'm actually going to go and change these passwords": Analyzing the Usability of Credential Audit Interfaces in Password Managers. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, Article 2, 13 pages. https://doi.org/10.1145/3613905.3650889

[47] Hyunho Kim, Boncho Ku, Jong Yeol Kim, Young-Jae Park, and Young-Bae Park. 2016. Confirmatory and exploratory factor analysis for validating the phlegm pattern questionnaire for healthy subjects. *Evidence-based Complementary and Alternative Medicine* 2016, 1 (2016), 2696019.

[48] Matthew Kosinski. 2024. What is a data breach? Accessed on 18.11.2024.

[49] David J. Kupfer. 2015. Anxiety and DSM-5. *Dialogues in Clinical Neuroscience* 17, 3 (2015), 245–246. https://doi.org/10.31887/DCNS.2015.17.3/dkupfer arXiv:https://doi.org/10.31887/DCNS.2015.17.3/dkupfer PMID: 26487805.

[50] Theodoros A Kyriazos and Anastasios Stalikas. 2018. Applied psychometrics: The steps of scale development and standardization process. *Psychology* 9, 11 (2018), 2531–2560.

[51] Rubén Daniel Ledesma, Pedro Valero-Mora, and Guillermo Macbeth. 2015. The scree test and the number of factors: a dynamic graphics approach. *The Spanish journal of psychology* 18 (2015), E11.

[52] Adrienn Lukács. 2016. What is privacy? The history and definition of privacy. (2016).

[53] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[54] Eetu Marttila, Aki Koivula, and Pekka Räsänen. 2021. Cybercrime victimization and problematic social media use: Findings from a nationally representative panel study. *American journal of criminal justice* 46, 6 (2021), 862–881.

[55] Oliver J Mason, Caroline Stevenson, and Fleur Freedman. 2014. Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *Frontiers in psychology* 5 (2014), 1298.

[56] Colleen McClain, Michelle Faverio, Monica Anderson, and Eugenie Park. 2023. How Americans view data privacy. *Pew Research Center* (2023).

[57] National Institute of Standards and Technology. Accessed on 20.01.2025. Cybersecurity Definition. NIST Glossary of Terms. https://web.archive.org/web/20241228233147/https://csrc.nist.gov/glossary/term/cybersecurity

[58] Goverment of Canada. 2025. Glossary. https://web.archive.org/web/20240724130659/https://www.cyber.gc.ca/en/glossary#c Accessed on 15.01.2025.

[59] Institute of Medicine (US), Board on the Health of Select Populations, and for Social Security Administration Disability Determinations Committee on Psychological Testing, Including Validity Testing. 2015. *Psychological testing in the service of disability determination.* National Academies Press.

[60] National Institute of Mental Health. 2024. Anxiety Disorders. https://web.archive.org/web/20241107205937/https://www.nimh.nih.gov/health/topics/anxiety-disorders Accessed on 7.11.2024.

[61] World Health Organization. 2023. Anxiety Disorders. https://web.archive.org/web/20241109132548/https://www.who.int/news-room/fact-sheets/detail/anxiety-disorders Accessed on 18.11.2024.

[62] Gábor Orosz, István Tóth-Király, and Beáta Bőthe. 2016. Four facets of Facebook intensity—the development of the multidimensional Facebook intensity scale. *Personality and individual differences* 100 (2016), 95–104.

[63] David W Putwain, Kristina Stockinger, Nathaniel P von der Embse, Shannon M Suldo, and Martin Daumiller. 2021. Test anxiety, anxiety disorders, and school-related wellbeing: Manifestations of the same or different constructs? *Journal of School Psychology* 88 (2021), 47–67.

[64] Murat Doğan Şahin. 2021. Effect of item order on certain psychometric properties: A demonstration on a cyberloafing scale. *Frontiers in psychology* 12 (2021), 590545.

[65] Steven F Sawyer. 2009. Analysis of variance: the fundamental concepts. *Journal of Manual & Manipulative Therapy* 17, 2 (2009), 27E–38E.

[66] Timothy M Scarella, Johannes AC Laferton, David K Ahern, Brian A Fallon, and Arthur Barsky. 2016. The relationship of hypochondriasis to anxiety, depressive, and somatoform disorders. *Psychosomatics* 57, 2 (2016), 200–207.

[67] Christopher R Sears and Daniel R Cunningham. 2024. Individual differences in psychological stress associated with data breach experiences. *Journal of Cybersecurity and Privacy* 4, 3 (2024), 594–614.

[68] John S Seberger, Marissel Llavore, Nicholas Nye Wyant, Irina Shklovski, and Sameer Patil. 2021. Empowering resignation: There's an app for that. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–18.

[69] MG Shahnawaz and Usama Rehman. 2020. Social networking addiction scale. *Cogent psychology* 7, 1 (2020), 1832032.

[70] Robert L Spitzer, Kurt Kroenke, Janet BW Williams, and Bernd Löwe. 2006. A brief measure for assessing generalized anxiety disorder: the GAD-7. *Archives of internal medicine* (2006).

[71] James Stevens et al. 2002. *Applied multivariate statistics for the social sciences*. Vol. 4. Lawrence erlbaum associates Mahwah, NJ.

[72] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 367–385. https://www.usenix.org/conference/soups2022/presentation/tang

[73] Mohsen Tavakol and Reg Dennick. 2011. Making sense of Cronbach's alpha. *International journal of medical education* 2 (2011), 53.

[74] R Jay Turner and Robyn Lewis Brown. 2010. Social support and mental health. *A handbook for the study of mental health: Social contexts, theories, and systems* 2 (2010), 200–212.

[75] Melanie Volkamer and Karen Renaud. 2013. Mental models – general introduction and review of their application to human-centred security. In *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, Berlin, Heidelberg, 255–280.

[76] Alexandra von Preuschen, Carolin Benda, Monika Christine Schuhmacher, and Verena Zimmermann. 2025. Fear, Fun or None: A Qualitative Quest Towards Unlocking Cybersecurity Attitudes. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 1–24.

[77] Alexandra Von Preuschen, Monika C Schuhmacher, and Verena Zimmermann. 2024. Beyond fear and frustration-towards a holistic understanding of emotions in cybersecurity. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 623–642.

[78] Yu-Yin Wang and Yi-Shun Wang. 2022. Development and validation of an artificial intelligence anxiety scale: An initial application in predicting motivated learning behavior. *Interactive Learning Environments* 30, 4 (2022), 619–634.

[79] Brett Williams, Andrys Onsman, and Ted Brown. 2010. Exploratory factor analysis: A five-step guide for novices. *Australasian journal of paramedicine* 8 (2010), 1–13.

[80] Anthony S Zigmond and R Philip Snaith. 1983. The hospital anxiety and depression scale. *Acta psychiatrica scandinavica* 67, 6 (1983), 361–370.

[81] Gregory D Zimet, Nancy W Dahlem, Sara G Zimet, and Gordon K Farley. 1988. The multidimensional scale of perceived social support. *Journal of personality assessment* 52, 1 (1988), 30–41.

A INSTRUCTIONS FOR THE SCALE

The scale was distributed with the following text:
The following questions are used for the development of a Cybersecurity Anxiety Scale. It consists of several statements.

Please indicate the degree to which you agree or disagree with each statement. In each case, make your choice in terms of how you feel **right now**, not what you have felt in the past or would like to feel.

Each item is measured on a 5-point Likert-type agreement scale (1=Strongly disagree, 2=disagree, 3=neutral, 4=agree, 5=Strongly agree). There are no right or wrong answers, so please answer honestly and thoughtfully.

B CONFIRMATORY FACTOR ANALYSIS (CFA) DIAGRAM

The diagram shows standardized estimates and standardized correlations among the latent factors for the finalized CybAS. Because the three factors are positively correlated, we think it is appropriate to calculate not just the factor scores but an average of all items for an overall CybAS score.

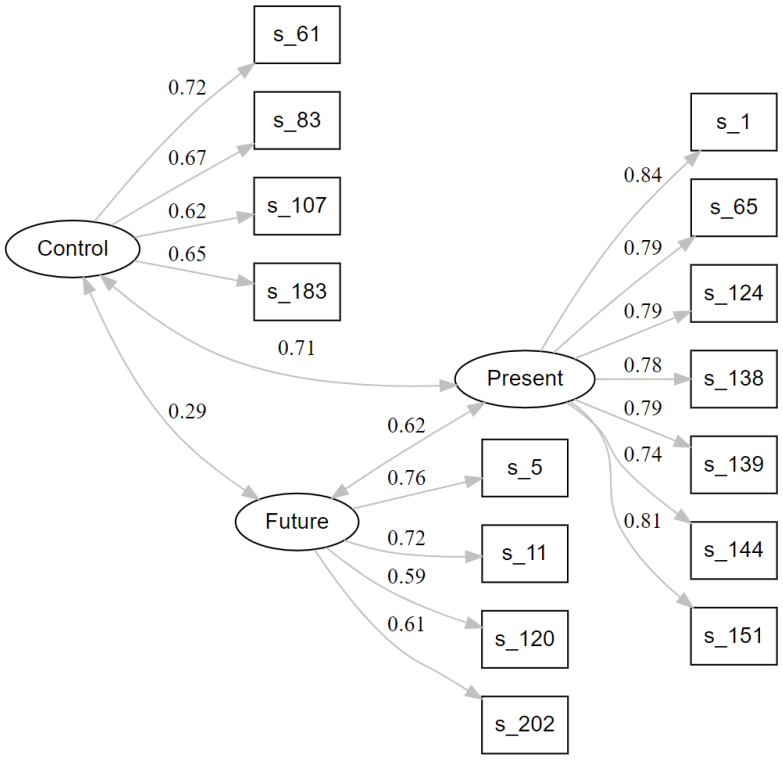

Figure 4: The diagram for the three-factor structure of the 15-item CybAS.

C NOMOLOGICAL NETWORK

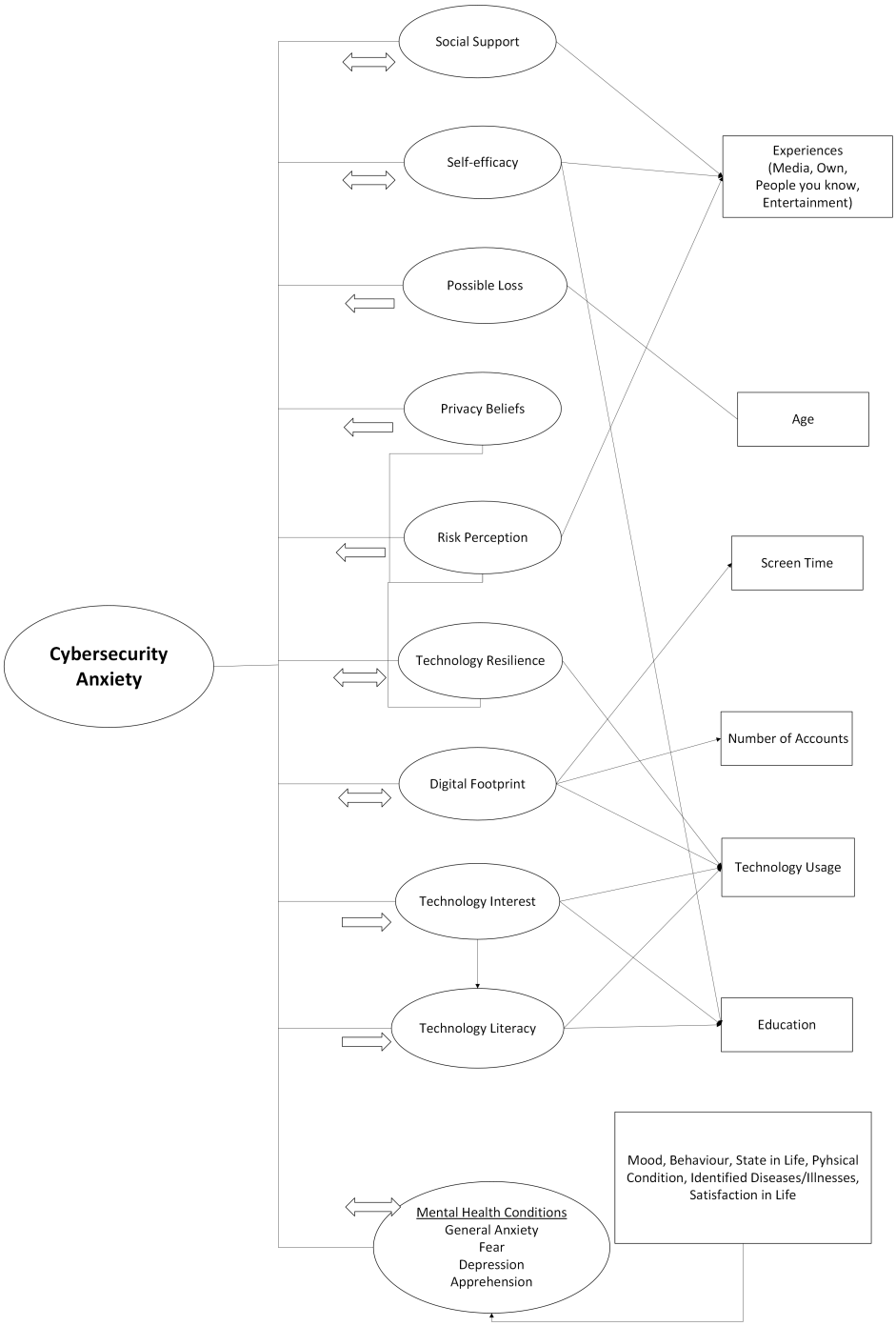

Figure 5: Nomological Network of Cybersecurity Anxiety

D SUPPLEMENTAL MATERIALS

Supplemental materials are available at:
https://anonymous.4open.science/r/CybAS-5607

Included are:

- Copy of the survey administered to participants
- Initial items and candidate items
- Variances by items for each data collection round
- Exploratory Factor Analysis (EFA) for the pilots and second round
- Item Response Theory (IRT) discrimination values and graphs