JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–10
https://doi.org/10.1093/cybsec/tyad007
Research paper

Research paper

Development of a new 'human cyber-resilience scale'

Adam N. Joinson [1,*], Matt Dixon [2], Lynne Coventry [2] and Pam Briggs [2]

[1]School of Management, University of Bath, BA2 7AY, Bath, UK and [2]Department of Psychology, Northumbria University, Newcastle upon Tyne NE1 8ST, UK

*Correspondence address. Information, Decision and Operations, School of Management, University of Bath, BA1 3PE, UK. Tel: +44-1225-383319; E-mail: A.Joinson@bath.ac.uk

Received 25 April 2022; revised 15 February 2023; accepted 3 April 2023

Abstract

While there has been an upsurge in interest in cyber resilience in organizations, we know little about the resilience of individuals to cyber attacks. Cyber resilience in a domestic or non-work setting is important because we know that the majority of people will face cyber threats in their use of technology across a range of contexts, and the ability to resist a cyber attack, or quickly recover and learn from a successful attack, is as important for individuals' wellbeing as it is for organizations. There is, unfortunately, a dearth of studies on the cyber resilience of people, in part because it is not clear how such a construct could be defined and then measured. In the present work, we present a series of five studies—with a total sample of $n = 1503$—that sought to develop and validate a theoretically based measure of cyber resilience for individuals. The final scale, comprising 16 items and 4 subscales (self-efficacy, learning and growth, social support, and helplessness), demonstrates good internal reliability and validity.

Introduction

In recent years, interest has grown in the concept of cyber resilience, capturing the ability of an organization to limit the consequences of cyber attacks and recover quickly following an incident, with a particular surge in research interest since 2016 [1]. However, the de-facto perspective of cyber resilience focuses on how systems and organizations can be cyber resilient. There is a distinct lack of research on what would constitute cyber resilience in individual users of technology who may encounter cybersecurity incidents in a domestic or non-work setting. Much of the organizational work focuses on the development of cyber-resilience frameworks (CRFs) that capture the key factors that mean an organization can both resist cyber attacks and recover swiftly from any adverse incident (see [2] for a systematic review). These frameworks generally follow a 'wave analogy' [3], which places a disruption event at the centre of a timeline and identifies factors prior to and after that event that can help mitigate or exacerbate the disruption. Within organizations, these include a priori factors that reduce the impact of an adverse event (e.g. situational awareness, good governance, and good security posture) and *post-hoc* factors that lead to swift recovery (e.g. ability to adapt, company's market strength, financial position, and social capital). With such frameworks, it becomes possible to measure organizational cyber resilience, and indeed a cyber-resilience self-assessment tool (CR-SAT) has been very recently proposed for small to medium-sized enterprises [4].

No such frameworks exist outside of the workplace, yet individuals and households face significant losses in the event of a cyber-attack. There has been a steady growth in cybercrime targeting the home environment, with the FBI reporting $10.2 billion losses in the USA in 2022 [5] and with PurpleSec reporting an average individual loss of 4476 USD [6]. The majority of victims are those aged >60 as these individuals may have retirement income but can be less cyber-aware. However, since the COVID-19 pandemic, the home worker has also become an important target for cyber attacks, meaning that the household has become a prime organizational attack vector [7].

It would therefore be useful to understand the factors that might help individuals and households effectively cope with and 'bounce back' from adverse events, something we refer to as 'human cyber resilience' to differentiate it from the organizational model. Over the past decade, there has been great interest in the way in which people manage security in the domestic environment (e.g. [8, 9]), and a variety of scales have been developed that measure how users perceive security threats, including their own vulnerability, or how severe certain incidents would be to them. Some scales also measure specific be-

haviours that would protect them from cybersecurity incidents, such as 'I use different passwords for different accounts that I have' [10], but there is little understanding about what factors underpin cyber resilience in general users. The organizational CRFs described above do not translate well to the domestic environment as factors such as governance, risk management, and training have little meaning for ordinary citizens, but there are other models of individual resilience (largely relating to health) that suggest that a cyber-resilient household would engage in good 'hygiene' behaviours (including proper password protection and making regular updates) in order to minimize the *likelihood* of an attack, take actions (backup regularly and adopt cyber insurance) that would minimize the *impact* of an attack, but also *learn*, either from their own mistakes or from knowledgeable others, so as to gradually improve their cyber defence in the longer term.

In this paper, we turn to a longstanding psychological resilience literature to develop a self-report measure of household cyber resilience. In keeping with the principles of the wave model, our aim is to understand what factors (attitudes, behaviours, skills, and resources) may help both reduce the likelihood of a cyberattack and also minimize the damage caused by any such attack. While there are obvious limitations in reliance on self-report to assess the resilience of individual users to cyber attack, the use of self-report is common to assess resilience in other settings (see below). While an individual's score on a self-report measure of resilience (whether cyber-related or other) may not predict precisely how that individual might respond to a particular attack or breach, at a population level it would be valuable in order to identify the factors that would underpin people's resilience to cyber breaches, and then allow for the testing of interventions (e.g. around training or response planning) that might help to improve citizen's resilience.

Resilience constructs and their relevance for cybersecurity

Resilience has been widely researched for many decades (e.g. [11–13]) and addresses the ability to cope positively with stress and adversity, including using stressors as a learning experience to develop oneself and better prepare for future challenges. Early resilience literature focussed on children raised in highly challenging situations (e.g. exposed to high levels of poverty, parental alcoholism, and/or parental mental illness, e.g. [12, 13]). Subsequent work has explored individual and group resilience in a wide range of contexts including the workplace (e.g. [14]), families (e.g. [15–18]), and elite sports (e.g. [19, 20]).

A number of scales exist that measure individual resilience, and these are reviewed by Pangallo et al. [21], who identified eight core constructs, which are consistently used in measuring resilience. These constructs are divided into whether they represent an internal or external resource that can be drawn on to support resilience. There are six internal resources, which can be seen as traits or characteristics of the individual (adaptation, self-efficacy, active coping, positive emotion, hardiness, and mastery), and two external resources, which support coping and recovery (supportive relationships and a structured environment).

At this point, we can begin to see some similarities that exist between the traditional resilience literature and the new literature on organizational cyber resilience. Both recognize a need for some kind of structured environment (good governance) and supportive relationships (social capital) and both recognize the importance of relevant skills and a means of adapting to change. If we now consider how we might measure resilience in the human-focused cybersecurity context, then we essentially take cybersecurity threat as the major stressor (see [22, 23]) and consider how the internal and external 'resilience' factors listed above might operate as candidate constructs in our scale development. In the following sections, we consider each factor in turn and discuss how it might manifest in a human cybersecurity context.

(1) *Adaptation*: Adaptation is the ability of an individual to respond productively to adversity by adjusting their thoughts and behaviours to meet the demands of a task. Previous literature has described adaptation as necessary to maintain homeostasis in the face of stressful conditions [24]. Importantly, *positive* adaptation is necessary for resilience [25], as adapting negatively may suggest unproductive coping strategies, including emotion focussed responses such as 'denial' of the situation [26]. It is likely that cyber-resilient individuals are those who are prepared to adapt positively to new and unexpected incidents. Cyber-resilient individuals should be able to learn from their mistakes and also accept that former behaviours and habits may have rendered them vulnerable to a cyber attack.

(2) *Mastery*: Mastery refers to an individual's actual ability to '*anticipate*, *manage*, *contain*, *or prevent the cognitive and emotional disruption that arises from* [*stressors*]' [27]. Mastery in cybersecurity terms links to digital literacy generally but is likely to include specific knowledge around cyber protection of accounts, data, and devices.

(3) *Self-efficacy*: Self-efficacy [28–30], also known as personal competence [24, 31–33], refers to a user's *perceived competence* in the digital space. This is likely to overlap with mastery, but crucially, if individuals perceive cybersecurity approaches to be beyond their skill level, then they will be unlikely to engage in cyber-resilient behaviours [34].

(4) *Positivity*: A positive outlook is one grounded in optimism, where the individual views adversity as something that can be approached and dealt with [35]. Positivity has long been considered an important component of resilience [25, 36–39], and it follows that positivity could work as a protective factor for individuals facing cyber incidents. Positive emotion is also important in fostering flexible thinking [40], which may be particularly useful when it comes to dealing with unfamiliar cybersecurity issues. Positivity is also crucial in taking a 'learning' approach to stressors, in that the user could use an incident to develop their knowledge or skills to prevent further incidents.

(5) *Perseverance* (*aka grit, hardiness, or tenacity*): Perseverance is an essential trait in dealing with chronic stressors or stressors that require a more extended or sustained response and has been integrated into several models of resilience [24, 41, 42]. It is typically measured as an individual's willingness to pursue goals and objectives in spite of adversity and setbacks. Cyber incidents may require perseverance as the time and effort required to ensure both protection and effective recovery can be onerous (e.g. backing data up regularly, updating, and remaining vigilant).

(6) *Active coping*: Active coping refers to the ability to consciously make use of the internal and external resources available to an individual when a stressor arises [43]. This includes behaviours such as reaching out to others to seek social support or making a conscious effort to consider one's own abilities to reassure themselves of their capability to deal with a problem. Active coping is essential for cyber resilience, implying that the more resilient user would be able to analyse the problem and deter-

mine the resources and processes necessary for action in the event of an adverse cyber incident.

(7) *Social support*: Social connections (friends, family, and colleagues) can protect against stress—they can help an individual maintain a positive outlook and the social network offers practical support [3, 8, 35]. Social support is highly relevant in the cybersecurity context, in terms of the network of people available to offer practical advice and also the longer-term sources of information that inform an individual's mental model of cyber threats and mitigation [44].

(8) *Structured environment*: A structured environment refers to regular and consistent behaviours and routines adopted by an individual. Early resilience work conducted by Werner [12] showed that a structured environment acts as an important protective factor in reducing the chaos of an individual's life. In the face of adversity, structure can act as an orderly counterbalance to the ensuing chaos. A structured environment in the cybersecurity context would imply good cyber hygiene, with routines set up in their digital environment around updates, backups, password protection, and orderly data storage.

These constructs regularly appear in the literature on psychological resilience, but also seem relevant as candidates for a human cyber-resilience scale, defined here as the ability to both resist and 'bounce back' from a cyber attack. However, it is not clear if all of the factors listed above will apply equally well to a human cyber-resilience context, so we are deliberately exploratory in our initial approach to scale development. Thus, while our eventual research goal is to develop and validate a measure of human cyber resilience, we also seek to investigate whether the same resilience factors as identified in other contexts also operate when considering a cybersecurity incident at an individual/human level.

In the sections below, we describe the process of adapting original scale items to be more appropriate for the cybersecurity context. In keeping with standard scale development protocols, we also engage in three processes: first, we use exploratory factor analysis to explore the relationships between items, identify subscales, and develop a set of candidate items for inclusion in a final scale; second, we use confirmatory factor analysis on a new sample to examine the relationship between the candidate items and the latent constructs (subscales) they contribute to measuring; and, finally, we investigate how well our scale aligns with other relevant measures.

Method

Item development

The initial 51 candidate items were developed by adapting items from a variety of existing general resilience scales [The Resilience Scale (RS), The Resilience Scale for Adults (RSA), the Connor–Davidson Resilience Scale (CD-Risc), Resilience in Midlife Scale (RIM), and the Brief Resilience Coping Scale (BRCS)] alongside the findings of Pangallo et al.'s review of resilience measures [21]. Individual items from each measure were extracted and considered for rewording to fit within a cybersecurity context and were explicitly worded to follow on from a prompt phrase of 'Thinking about my experiences with online cybersecurity threats or issues (being hacked, phishing, etc) …'. Following this process, the first version of the measure was produced, consisting of 51 candidate items (see Supplementary Appendix A).

Studies 1–3: exploratory factor analysis and scale refinement

Three separate studies were used to explore the underlying structure amongst the items identified to reduce the potential number of items comprising the scale (and subscales) based on the coherence of the factors/items, and (where needed) to develop and test new items. Across the three studies, the same broad statistical approach was used with some minor variations. In Study 1, the exploratory technique of principal axis factoring (PAF) was used because we did not know either if the data/scales would be normally distributed or the number of factors that would be extracted—and PAF is recommended for non-normally distributed data [45]. In all subsequent studies, maximum likelihood was used because the scales were relatively normally distributed, and MLE has a number of advantages over PAF [46] including the ability to examine inter-factor correlations and calculate fit indices [45].

Promax rotation was used because, although it is an oblique rotation technique (i.e. the factors are assumed be correlated), it increases the likelihood that a 'simple structure' will be obtained by first calculating a varimax rotation (which assumes no correlation between factors), and then applies a transformation that maximizes higher loadings and minimizes smaller cross-loadings [47–49]. Across the first three studies, the next step was to examine the Kaiser–Meyer–Olkin (KMO) Measure of Sampling Adequacy and Barlett's test of sphericity to check whether the data were suitable for dimensionality reduction. These tests look for the degree to which items are correlated in the data set (and therefore can, in principle, be reduced to fewer dimensions), and typically KMO should be above 0.6 [47], and the χ^2 from Bartlett's test should be significant. Next, the eigenvalues for the extracted factors were examined to determine the number of factors to be interpreted. Although it is justifiable to extract all factors with an eigenvalue >1, a more common method is to look for the 'elbow' in a scree plot (effectively where the proportion of variance explained by each additional factor levels off). This led to an initial five factors being initially investigated in Study 1 (see Supplementary Appendix B for the scree plot), which was reduced to four due to the final factor being incoherent and uninterpretable. In Studies 2 and 3, the number of factors extracted was limited to a maximum of four. Next, the communality scores for the items were examined. The communality score expresses the degree to which the variance within an item is explained by the component(s) it loads on, and correlations with other items. A general rule of thumb is that a communality score should be >0.4, and anything lower should be looked at particularly closely [45]. In some cases, we retained items with a communality <0.4 if they loaded cleanly on a factor and were needed to maintain a minimum number of items on the factor (four), and removed items with a communality above 0.4 if there were too many items on a factor, or there was considerable overlap with other (retained) items.

Finally, any items with cross loadings (defined as >0.3, and at least half the size of the main loading), or low primary loadings (<0.4) were removed from the item set.

The sample characteristics and item development approach for Studies 1–3 are summarized in Table 1. In all three studies, an attention check item was included in the survey ('It is important that you are paying attention. Please select "strongly agree"'). The data from participants who failed the attention check were removed from the analysis. All participants were recruited using the platform Prolific (https://www.prolific.co), and paid for their participation. Prolific provides access to around 130 000 verified study participants who are paid for completion of research studies. The platform al-

Table 1: Summary of Studies 1–3.

	Study 1	Study 2	Study 3
Sample size (*n*)	273	326	174
Mean age years (SD)	31.71 (11.14)	32.63 (10.94)	32.06 (11.73)
Sample *N*: males/females/other	135/138/0	167/156/1	50/123/1
Factor analytic technique/rotation	PAF/PROMAX	MLE/PROMAX	MLE/PROMAX
KMO	0.91	0.91	0.79
Bartlett's test of sphericity	$\chi^2 = 6706.28$, df = 1275, $P < 0.000$	$\chi^2 = 4262.35$, df = 350, $P < 0.000$	$\chi^2 = 1257.49$, df = 120, $P < 0.000$
Item development steps	51 items examined; 28 items retained on first 4 factors; 6 additional items removed based on simple structure rules and loading size; 4 new items added for Study 2 and 1 original item reversed	26 items examined; 21 items retained (4 factors); reduced to 16 items (4 per subscale) for Study 3 based on item overlaps, loadings, and communalities.	16 items examined; 15 items retained (4 factors—1 item removed due to cross loadings); 3 candidate replacement items developed for Study 4.

lows for filtering based on a range of demographic variables (e.g. location, first language, and gender). In Studies 1–4, the geographic filter was set to UK and Ireland. All studies were submitted, and received a favourable response, from the Psychology Ethics Committee of Northumbria University.

In the initial Study 1, 11 factors had eigenvalues >1. However, inspection of the scree plot suggested that four or five would be the optimal number to extract using the 'elbow' of the plot as a guide. Close examination of the items loading on the factors suggested that the fifth factor was not interpretable due to the small number of items loading on it, so a four-factor, 28-item solution was adopted. Some items had lower than ideal communalities (see Supplementary Appendix B, Table 2)—mostly the items loading on the third factor that seemed to reflect a positive, learning approach to a cyber breach. Because they cohered around a distinct factor, these items were retained for the next study. Other items were removed on the basis of either lower loadings than other items, or overlap between items. For instance, the item 'I know how to protect my accounts' was removed because of overlap with similar items (e.g. 'I know how to protect my devices'). Some items with lower communalities were retained for Study 2 because they drew on different aspects of resilience, and so allowed for a broader interpretation of the dimensions.

An initial scan of the factors and items (alongside their original construct) suggested that the items did not form around the original constructs. Instead, the first factor was comprised primarily of items associated with self-reliance and training, the second factor comprising protective routines and knowledge, the third comprising items expressing adaption and positive thinking, and the final factor comprised items around social support. However, the number of items loading on the factors was uneven, with 11 items loading on the first factor, followed by 8 on factor 2, 5 on factor 3, and 4 on factor 4. In order to rebalance this for scale development, a second round of item development and exploratory factor analysis was conducted (Study 2), with new items developed in order to better represent the underlying structure of the scale found in the first study, and re-balance the item composition by adding some reversed items.

In order to develop the items for Study 2, the items with the greatest loading and interpretational coherence from each factor were selected for completion by a new sample of participants, alongside new items expected to load on factors 2–4. This led to a total of 26 items, identified as corresponding to self-reliance (eight items), social support (six items), protective routines and knowledge (six items), and adaptability and positive thinking (six items). In order to address potential issues with response sets, seven items were reversed.

Interpretation of the pattern matrix from Study 2 showed that the first factor again contained the majority of items, with both self-reliance and protective routine items loading on it. After studying the items comprising this factor, it is henceforth termed 'self-efficacy' since the items represent both mastery and knowledge. Factor 2 was comprised of the social support items, and Factor 3 contained four items that—while drawn from different initial subscales—seemed to suggest helplessness in the face of threat. The final factor contained three of the adaption and positive thinking items, all relating to the interpretation of a cyber threat as an opportunity for learning and growth. To test these interpretations, a 'self-efficacy' subscale was created by selecting the items with the highest loadings from Study 2 that represented efficacy rather than routine, and additional learning and growth items and helplessness items developed for testing in Study 3.

Study 3 was conducted to test the new subscales, with four items per scale. Four items were selected to measure 'helplessness', and an additional item ('I can use the experiences to improve') added to the 'learning and growth' subscale. The rotated solution (pattern matrix) is shown in Table S4 in Supplementary Materials, Appendix B.

Interpretation of the loadings showed strong support for the conclusions of the previous study, with self-efficacy (Factor 1), social support (Factor 2), learning and growth (Factor 3), and helplessness (Factor 4) emerging as interpretable factors comprising items with minimal cross loadings. A single item ('I don't know what to do first') had a significant cross loading on the efficacy and helplessness factors. In the final iteration of item development (Study 4), this item was replaced with three candidate items—'it's easy to feel overwhelmed', 'they feel like impossible problems', and 'I feel helpless', with the intention to select the most appropriate for confirmatory factor analysis.

Study 4

In Study 4, the items comprising the self-efficacy, social support, and learning and growth subscales, along with the three original helplessness items and three new candidate items were completed by 161 Prolific participants. Following removal of those who incorrectly answered the attention check question ($n = 10$, same question as in

Table 2: Pattern matrix, Study 4.

Item	1	2	3	4
I have friends/family who can help me deal with the threats			− 0.632	
I have people who can support me while I deal with the issue			− 0.625	
I don't have any technically minded friends who can help me			0.884	
I don't have any one I can turn to for support			0.879	
I see them as learning experiences				0.727
The experiences help me learn how to cope under pressure				0.731
I view them as challenges				0.737
I can use the experiences to improve				0.567
They feel like impossible problems		0.734		
I give up when the issues look too hard to solve		0.507		
I am easily discouraged by failure		0.546		
I don't see the point in trying		0.836		
I feel helpless		0.785		
I can keep my devices secure	0.689			
I believe in myself to deal with it	0.778			
I am good at dealing with issues like this	0.848			
I know that I can solve most security problems	0.91			

Studies 1–3), the final sample was 151 (57 male, 83 female, 1 prefer not to say). All resided in the UK. The average age of the respondents was 37.45 years (SD = 14.19).

To select the most appropriate new helplessness item for confirmatory factor analysis, a final exploratory factor analysis using maximum likelihood with promax rotation was conducted to examine communalities and loadings. Bartlett's test of sphericity (χ^2 = 1262.61 (df 153), P < 0.000) and KMO measure of sampling adequacy (0.85) indicated that the data was suitable for factor analysis. One helplessness item ('It's easy to feel overwhelmed') had a communality <0.3, so was removed from further analysis, leaving the two new items as viable additions to Factor 2. Analysis of the pattern matrix found that all items loaded as expected on factors representing the subscales, with all five helplessness items loading on a single factor without any cross loadings (see Table 2). The inter-factor correlation matrix is shown in Table 3.

In order to examine the relationship between the items and the latent (subscale) variable, confirmatory factor analysis was conducted using AMOS (Version 26). Using this approach, the candidate additional helplessness item 'I give up when the issues look too hard to solve' showed the lowest relationship with the latent variable, so was removed to leave four remaining helplessness items. Analysis of the goodness of fit indices showed an acceptable fit: RMSEA was 0.06, which is at or below the recommended cut-off point. The CFI (0.952) and TLI (0.94) were both above the cut-off point (higher indicating a better fit) suggested by Netemeyer and colleagues of 0.9 [50].

The confirmatory factor analysis provided support for the development of four subscales, each comprising four items reflecting self-efficacy, helplessness, social support, and learning and growth, respectively, and each measured on a five-point Likert scale scored such that Strongly Disagree = 1 and Strongly Agree = 5. Note that a high score on the helplessness scale is indicative of poor resilience, whereas a high score on the other subscales indicates strong resilience. Thus, when using the instrument to generate an overall human cyber-resilience score, the helplessness items should be subtracted from the overall scale. Cronbach's alpha and standardized regression weights for the final items and subscales are shown in Table 4.

Study 5

The goal of the final study was to compare scores on the cyber-resilience measure across three (primarily) English speaking countries and to examine the convergent and discriminant validity of the scale by correlating the cyber-resilience subscale with existing measures of general resilience, computer self-efficacy, and cybersecurity behaviour. For this purpose, we chose the Security Behaviour Intentions Scale (SeBIS) [10] as a security behaviours measure, the Brief Resilience Scale [51], and The Computer Self-Efficacy Measure [37]. We expected each of the subscales to correlate with the measure of general resilience, and the self-efficacy and helplessness subscales to correlate with general computer self-efficacy. We expected a positive correlation between self-efficacy and security intentions (SeBIS), and a negative correlation between helplessness and SeBIS. To test the relationship between human cyber resilience and the stress caused by cybersecurity victimization, we additionally asked people whether they had experienced a range of breaches/cybersecurity events, and to score the amount of stress caused. We predicted a negative correlation between overall human cyber resilience and the stress caused by victimization, and a positive correlation between the helplessness subscale and cyber victimization stress.

Participants

A total of 617 participants were recruited using the Prolific panel. Of these, 33 were removed for failing the attention check, and 5 for not ticking the consent form, or withdrawing consent. This left a final sample of 579 people, 236 of whom were male, 340 female, and 3 other gender. The geographic distribution of participants was 152 in Canada, 275 in the UK, and 152 in the USA. The mean age of the sample was 33.86 years old (SD = 11.80, range 18–82).

Measures

Human cyber-resilience scale

Following scale development in studies 1–4, above, the final human cyber-resilience scale comprises 16 items across four subscales: self-efficacy (α = 0.83); social support (α = 0.86); helplessness (α = 0.73);

Table 3: Factor correlation matrix (using factor scores), Study 4.

Factor	1 (self-efficacy)	2 (helplessness)	3 (social support)	4 (learning and growth)
1 (self-efficacy)	1	−0.62	−0.25	0.42
2 (helplessness)	−0.62	1	0.39	−0.33
3 (social support)	−0.25	0.39	1	−0.22

Table 4: Final items, human cyber-resilience scale with standardized regression weights and Cronbach's alpha.

Subscale	Item	β	Cronbach's alpha
Self-efficacy	I can keep my devices secure	0.67	0.89
	I believe in myself to deal with it	0.84	
	I am good at dealing with issues like this	0.89	
	I know that I can solve most security problems	0.85	
Helplessness	I am easily discouraged by failure	0.63	0.82
	I don't see the point in trying	0.65	
	I feel helpless	0.80	
	They feel like impossible problems	0.87	
Social support	I have friends/family who can help me deal with the threats	0.62	0.88
	I have people who can support me while I deal with the issue	0.64	
	I don't have any technically minded friends who can help me (R)	0.90	
	I don't have any one I can turn to for support (R)	0.85	
Learning and growth	I see them as learning experiences	0.70	0.79
	The experiences help me learn how to cope under pressure	0.74	
	I view them as challenges	0.74	
	I can use the experiences to improve	0.63	

and learning and growth ($\alpha = 0.63$).[1] Cronbach's alpha of the overall scale (with the helplessness items reverse-scored) was 0.84. Items are responded to using the prompt 'Thinking about my experiences with online cybersecurity threats or issues (e.g. being hacked, phishing, etc.)': using a five point Likert-type scale anchored at 'Strongly disagree', 'Somewhat disagree', 'Neither agree nor disagree', 'Somewhat agree', and 'Strongly agree'.

Security Behaviour Intentions Scale

The SeBIS scale comprises 16 items designed to measure people's security intentions across four domains: device securement (e.g. 'I use a PIN or passcode to unlock my mobile phone'); password generation (e.g. 'I use different passwords for different accounts I have'); proactive awareness (e.g. 'When browsing websites I mouseover links to see where they go, before clicking them'); and updating (e.g. 'I try to make sure that the programs I use are up-to-date'). Each item is responded using a scale anchored at 'never', 'rarely', 'sometimes', 'often', and 'always'.

1 Cronbach's alpha for the learning and growth subscale was lower than that found in Study 4. Further analysis identified one item ('I view them as challenges') that confirmatory factor analysis showed to have a lower connection to the latent variable (0.29). Further investigation showed that this could not be explained by geographic differences in responses to the items, and re-testing and re-examination of earlier analyses confirmed it to be consistently associated with the learning and growth subscale. Looking at the original survey, we noted that item randomization in this study occurred by block rather than all items, and the item 'I view them as challenges' was surrounded by items expressing negative views towards participants' ability to respond to a cyber threat. We interpret this as suggesting that—for some participants—this design artefact in the survey may have led to a more negative interpretation of the word 'challenges' than in previous implementations of the scale. As such, we retained the item, but would caution that items should be presented in a randomized order in the future.

Brief Resilience Scale [51]

The Brief Resilience Scale is a simple six-item measure of the ability of individuals to bounce back using a six point Likert scale. Example items include 'I tend to bounce back quickly after hard times' and 'It does not take me long to recover from a stressful event'. Items were responded to using a five point Likert-type scale anchored at 'Strongly disagree', 'Somewhat disagree', 'Neither agree nor disagree', 'Somewhat agree', and 'Strongly agree'.

Computer Self-Efficacy Scale

Howard's Computer Self-Efficacy Scale [37] is a 12-item unidimensional scale that includes items such as 'I am confident that I could deal efficiently with unexpected computer events', 'I can usually handle whatever computer problem comes my way', and 'I can persist and complete most any computer-related task'. Items were responded to using a five-point Likert-type scale anchored at 'Strongly disagree', 'Somewhat disagree', 'Neither agree nor disagree', 'Somewhat agree', and 'Strongly agree'.

Cyber-security victimization

Participants were instructed that: 'The following questions are about your experiences of cyber-security victimization. Please use the slider for any that apply and indicate how stressful you found the experience. If any do not apply to you, please tick the Not Applicable box at the end of the slider'. The five scenarios were as follows: (1) I have lost money; (2) I have lost data (photos, files, etc.); (3) I have had a virus; (4) My email has been compromised; (5) I had to buy a new device; and (6) My social media accounts have been hacked. Participants used a slider (running from 0 to 100) anchored at 'Not at all stressful' and 'Very Stressful' to respond or ticked 'Not applicable' if they had not experienced that cybersecurity event.

Table 5: Pearson correlations between cyber-resilience scales and related constructs ($n = 565$–576 based on pairwise removal).

Scale	SeBIS	General resilience	Computer self-efficacy	Self-efficacy	Social support	Helplessness[a]	Learning and growth
SeBIS	1	0.25**	0.37**	0.37*	0.09*	−0.33**	0.28**
General resilience	0.25**	1	0.22**	0.21**	0.14**	−0.39**	0.20**
Computer self-efficacy	0.37**	0.22**	1	0.77**	0.09*	−0.56**	0.40**
Self-efficacy	0.37**	0.21**	0.77**	1	0.19*	−0.62**	0.47**
Social support	0.09*	0.14*	0.09*	0.19*	1	−0.30**	0.17**
Helplessness[a]	−0.33**	−0.39**	−0.56**	−0.62**	−0.30**	1	−0.34**
Learning and growth	0.28**	0.20**	0.40**	0.47**	0.17**	−0.34**	1
Overall cyber-resilience scale[b]	0.37**	0.33**	0.62**	0.77**	0.64**	−0.78**	0.64**

[a]Helplessness items not reversed when treated as a subscale for interpretational ease.

[b]Overall scale score computed by summing the scores on the self-efficacy, social support, and learning and growth subscales, and subtracting the helplessness subscale; * $P < 0.05$, ** $P < 0.001$.

Results

In order to test concurrent validity, each of the human cyber-resilience subscales—as well as the overall human cyber-resilience scale—was correlated with SeBIS alongside the measures of general resilience and computer self-efficacy. As predicted, efficacy correlated positively, and helplessness negatively, with SeBIS, the measure of general resilience and computer self-efficacy. The social support subscale showed a low positive correlation with all three comparison scales, while the learning and growth subscale correlated positively with both computer self-efficacy and generalized resilience (see Table 5).

We interpret this pattern of results as supporting the notion that the different parts of the cyber-resilience scale demonstrate concurrent validity in that they correlate as expected with constructs that should conceptually be related to the different components of the scale. For instance, the strongest positive relationship is between our human cyber-resilience self-efficacy subscale and the measure of overall computer self-efficacy. The pattern also supports our view that the scale can be treated as either a single overall measure (by reversing helplessness and calculating an overall mean), or as four subscales. In part, this will depend on the nature of the research question (e.g. when social support is of interest in itself). The positive correlations between our human cyber-resilience scale (and subscales) and general resilience is as expected, but relatively small (0.33), suggesting that ∼10% of the variance in human cyber resilience can be accounted for by general levels of resilience. This suggests that as a construct, human cyber resilience will be useful above and beyond general resilience. Similarly, SeBIS and human cyber resilience show a positive overall correlation, but the shared variance is relatively low (around 14%), suggesting that cyber resilience is a related, but separate construct to Security Behaviour and Intentions.

Human cyber resilience and cybersecurity victimization

Rates of victimization varied across the events we measured, with having a virus reported by a majority of participants ($n = 434, 75\%$), while 142 (25%) reported losing money, and 134 (23%) reported having to buy a new device. The correlations between the experience of stress related to each cyber vicitimization type and human cyber resilience are shown in Table 6.

As would be expected, there is a general trend of a negative correlation between overall human cyber resilience and the stress experienced following common cybersecurity victimization. So, as resilience (as measured by the human cyber-resilience scale) increases, so the stress reported from common cyber breaches/victimization decreases. This provides strong evidence for the utility and validity of the self-report measure we have developed, and suggests that if we are to increase people's cyber resilience in the face of common threats, we need to address not only the skills needed (efficacy), but also the understanding that these skills will help protect the user and provide learning experiences.

Demographic comparisons

We next wished to examine any relationship between the level of cyber resilience and the demographic characteristics within our sample. We did this in order to provide contextual data for future use, as well as to explore if aspects of cyber resilience were likely to be influenced by cultural and other demographic differences (while acknowledging cultural similarities in our sample countries).

A MANOVA—using the country of residence as the independent variable and our four cyber-resilience subscales as dependent variables—found an overall effect of country across the scales [F (8, 1122) = 2.32, $P = 0.02$]. Analysis of the between subjects effects showed that this difference was driven by differences in scores on the learning and growth subscale [F (2, 563) = 3.37, $P < 0.05$]. The other three scales did not show a significant difference by country. Subsequent post-hoc tests revealed that participants in the USA and Canada (means 3.60 and 3.59) scored marginally significantly higher ($P < 0.1$) than UK-based respondents (mean = 3.45) in their scores on the 'learning and growth' subscale.

Analysis by gender using the same method found a significant overall effect [F (8, 1124) = 13.60, $P < 0.001$], with significant between-subjects effects for all scales (see Table 7).

Across the subscales, males reported greater resilience in terms of efficacy and learning and growth, while females reported greater resilience via social support, and lower resilience through increased helplessness. The gender differences for efficacy and helplessness replicate previous findings in reported efficacy in cybersecurity settings (e.g. [39]), but of course may not represent actual differences in resilience or skills.

Finally, we correlated our four component scales with age, but found no (linear) relationship for any of the scales (r_s ranged from −0.06 to 0.03, all Ps > 0.10).

Discussion

Organizational cyber resilience has become a 'hot topic' in the cybersecurity literature with a great deal of attention now devoted to the organizational pillars of resilience (e.g. the ability to anticipate, monitor, respond to, and learn from adverse events—[52]). Recently, Kott and Linkov [53] have made a plea for better tools to measure

Table 6: Pearson correlations between cyber-resilience scales and stress caused by cyber victimization.

Cyber victimization stress experienced (*n*)	Self-efficacy	Social support	Helplessness	Learning and growth	Overall cyber resilience
I have lost money ($n = 142$)	−0.15	−0.11	0.28**	−0.16	−0.26**
I have lost data (photos, files, etc.) ($n = 211$)	−0.11	−0.08	0.16*	−0.14*	−0.18**
I have had a virus ($n = 434$)	−0.31**	−0.10*	0.29**	−0.07	−0.27**
My email has been compromised ($n = 258$)	−0.06	0.04	0.11	0.09	−0.01
I had to buy a new device ($n = 137$)	−0.20*	−0.30**	0.32*	−0.22*	−0.37**
My social media accounts have been hacked ($n = 207$)	−0.12	0.01	0.28**	0.15	−0.13

*$P < 0.05$, **$P < 0.01$.

Table 7: Human cyber resilience by gender (three people selecting 'other' or 'non-binary' excluded from the analysis).

Cyber-resilience subscale	Males (M, SD)	Females (M, SD)	Univariate tests
Self-efficacy	3.93 (0.49)	3.32 (0.41)	$F\ (1, 562) = 84.49, P < 0.001$
Social support	3.58 (0.64)	3.75 (0.53)	$F\ (1, 562) = 4.46, P = 0.035$
Learning and growth	3.66 (0.44)	3.43 (0.37)	$F\ (1, 562) = 16.22, P < 0.001$
Helplessness	2.02 (0.49)	2.48 (0.41)	$F\ (1, 562) = 51.34, P < 0.001$

resilience. They argue that the few existing attempts to measure cyber resilience focus on the ability of systems to resist well defined and predictable threats (i.e. measure the probability that systems will fail in response to different threat scenarios). This omits a key component of resilience, which is the ability to learn from experience and develop the capacity to respond to unknown future events. Again, Kott and Linkov are talking here about better measurement of organizational cyber resilience, but the need for measurement exists outside of the workplace. In short, while our understanding of organizational resilience is growing rapidly, our understanding of the factors that impact individual (and/or household) cyber resilience has lagged behind and our ability to measure individual cyber resilience is entirely missing from the literature.

In this paper, we have developed a measure of individual cyber resilience (i.e. resilience outside of the workplace) that has both divergent and convergent validity (i.e. that it measures something distinct, but relates meaningfully to relevant, established scales). We have shown that this scale relates meaningfully to a more general measure of resilience (Smith et al.'s Brief Resilience Scale [51]), to computer self-efficacy [37], and to Egelman and Peer's widely used SeBIS [10], which is what we would expect. Additionally, we have shown that our measure correlates with the reported stress experienced across a range of common cyber security victimization events. Using the reported stress experienced as a proxy for the impact and difficulty dealing with victimization, this suggests that our measure is actually measuring individual cyber resilience, and would be useful in predicting the likely impact of victimization, and in the planning of specific interventions to support positive recovery.

Our scale has four subcomponents: self-efficacy, social support, learning and growth, and helplessness and so it is useful to understand how these subscales might map onto the wider cyber security literature. Certainly, two of our subscales (self-efficacy and learning and growth) resonate well with the established cyber security literature (and also the literature on organizational cyber resilience more generally). For example, self-efficacy is a known factor in predicting an individual's ability to respond to cyber threat (e.g. [34, 54]) and learning and growth is a key component of the CR-SAT [4], which recognizes that, in a cyber-resilient organization, adverse incidents become opportunities for learning.

The two other subscales (social support and helplessness) are telling us something rather new. First, social support as a measure is interesting as it recognizes that low individual cybersecurity capability can be compensated for by a social network of more knowledgeable individuals. In other words, those with poor cybersecurity self-efficacy may find a path to resilience with the help of others. Where those others are absent (in individuals who are more socially isolated or who surround themselves with individuals who are similarly unsure of how to protect themselves), then resilience may be lowered. This observation ties in with a very recent literature that talks about the importance of knowledgeable individuals in a network of influence. In the last 2 years, for example, research papers have emerged that describe a new role for 'cyberguardians' or cybersecurity champions in an organizational or community network. They clearly show that gains can be made by the presence of knowledgeable individuals who can spread understanding of cybersecurity within their peer network, and this is true both within the workplace (e.g. [55]) and within local communities (e.g. [56–58]).

Helplessness is another interesting subscale. Its role within the general resilience literature relates to the kinds of coping strategies people will adopt under difficult circumstances. In particular, when a threat is severe but an individual has limited capacity to deal with that threat, then they may adopt a dysfunctional coping strategy, which may mean engaging in denial (assuring themselves that the threat is not that severe) or simply burying their head in the sand and refusing to engage. Again, we can see some discussion of this in very recent literature on cybersecurity disengagement and security fatigue. For example, Morrison et al. [59] described cybersecurity disengagement taken as a deliberate strategy for older adults who felt helpless in the face of evolving cyber threats. Further, Reeves et al. [1] describe 'attitudinal' cybersecurity fatigue, which manifests itself as emotional exhaustion or moral disengagement—i.e. individuals no longer care about doing the right thing, in part because they feel they simply cannot keep up or cope. The focus of many cybersecurity awareness campaigns on the myriad threats users face rather than on informa-

tion to build a sense of self-efficacy and control is likely to exacerbate a sense of helplessness [60].

The scale can be used to give a holistic measure of human cyber resilience (with the helplessness subscale reverse-scored) and could be used to make meaningful demographic comparisons against age, gender, ethnicity, etc. or could be used to give an overall measure of cyber resilience at time 1 and time 2, following a campaign or intervention. The subscales can then be used to understand the component factors giving rise to resilience within a particular demographic, thus giving useful data to inform the design of future interventions. This is useful when we consider, for example, a recent literature that shows that feelings of competence are important to offset the anxieties and feelings of helplessness caused by cyberthreat (e.g. [54, 61]).

Future directions

Given the paucity of research on cyber resilience outside of the work setting, it is important that further research be conducted into the development of human cyber resilience, including investigation of the protective factors that contribute to this resilience, and the processes involved in the development of cyber resilience. The field would benefit from both qualitative and quantitative investigations of individuals's ability to recover from cyber incidents and the effectiveness of different protective strategies. It is notable that, while we have offered a means to measure self-rated cyber resilience and shown how this correlates with self-rated cybersecurity knowledge and behaviours (SeBIS), we have *not* shown its relationship to the actual performance of those individuals subjected to a cyber attack and their ability to recover from such an attack. Such work is difficult to do in an individual setting, but one possible compromise might be to explore those working from home, where workplace vulnerability measures could be calibrated against our human cyber-resilience scale.

Cybersecurity experts need to assess the effectiveness of different protective measures and develop innovative prevention and intervention programmes that build on people's cyber-resilience strengths and increase protective factors, as well as address problematic areas. For instance, we reported a series of relationships between the efficacy and helplessness subscales and experienced stress following a cyber attack or event. Under our definition that resilience is not only hardness against attack, but also the ability to recover following victimization, then interventions could focus on techniques that reduce a sense of helplessness and help speedy recovery (e.g. by using cloud backups or remote deletion to secure devices). The human cyber-resilience scale could be used to identify subgroups in order to target an intervention, or to measure the effectiveness of an intervention over a longer period of time. Such efforts may not only enhance the cyber resilience of individuals, but potentially reduce the harm caused by future cyber incidents.

Conclusions

Digitization has put cyber concerns at the heart of our everyday lives. Cyber incidents can massively impact our everyday lives, making it crucial to improve our ability to both assess and develop individual cyber resilience. Here, we have presented a human cyber-resilience scale with four sub-components: self-efficacy, social support, learning and growth, and helplessness The scale can be used to better understand the landscape of human cyber resilience and to ensure that individuals and households can effectively deal with the stresses, challenges, and changes accompanying increased digitization of our lives outside of work. The human cyber-resilience scale is a brief, self-rated measure of cyber resilience that has sound psychometric properties. It can be used as a multidimensional construct, or can be used to assess which of the four underlying factors is most critical in a particular context. Prevention and intervention programmes could focus on developing these protective factors. The scale could also be utilized in research settings to compare the effectiveness of different interventions, in terms of behaviour change that not only minimizes the likelihood of a cyber attack in the short term, but also captures a willingness to engage in cybersecurity learning and seek out support networks in the longer term.

Supplementary data

Supplementary data is available at *Cybersecurity Journal* online.

Funding

This work was supported with funding from EPSRC to A.J., L.C., and P.B. as part of the 'Cybersecurity across the Lifespan' (cSALSA) project (EP/P011454/1, EP/P011446/1).

Conflicts of interest

No conflicts of interest were reported.

Author contributions

Adam N. Joinson (Conceptualization [equal], Data curation [lead], Formal analysis [lead], Funding acquisition [lead], Methodology [lead], Project administration [equal], Writing – original draft [lead], Writing – review & editing [equal]), Matt Dixon (Data curation [equal], Methodology [equal]), Lynne Coventry (Conceptualization [equal], Funding acquisition [supporting], Writing – original draft [supporting], Writing – review & editing [supporting]), and Pam Briggs (Conceptualization [equal], Investigation [equal], Methodology [equal], Writing – original draft [supporting], Writing – review & editing [supporting])

References

1. Reeves A, Delfabbo P, Calic D. Encouraging employee engagement with cybersecurity: how to tackle cyber fatigue. *SAGE Open* 2021;**11**:1–14.
2. Sepúlveda Estay DA, Sahay R, Barfod MB. *et al.* A systematic review of cyber-resilience assessment frameworks. *Comput Secur* 2020;**97**:101996.
3. Sepúlveda Estay DA, Guerra P. The wave analogy of resilience as applied to shipping operations. *Cybersecur Resil Arctic* 2020;**58**:265–73.
4. Carias JF, Arrizabalaga S, Labaka L. *et al.* Cyber resilience self-assessment tool (CR-SAT) for SMEs. *IEEE Access* 2021;**9**:80741–62.
5. Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (4 April 2023, date last accessed).
6. PurpleSec. Cyber Security Statistics. https://purplesec.us/resources/cyber-security-statistics/#Cybercrime (4 April 2023, date last accessed).
7. Verizon. Mobile Security Index 2022. https://www.verizon.com/business/resources/reports/2022-msi-report.pdf (17 November 2022, date last accessed).
8. Dumont M, Provost MA. Resilience in adolescents: protective role of social support, coping strategies, self-esteem, and social activities on experience of stress and depression. *J Youth Adolesc* 1999;**28**:343–63.
9. Thompson N, Hoffman L, Chen R. *et al.* 'Security begins at home': determinants of home computer and mobile device security behavior. *Comput Secur* 2017;**70**:376–91.
10. Egelman S, Peer E. Scaling the security wall: developing a security behavior intentions scale (SeBIS). In: Proceedings of ACM Conference on Human Factors in Computing Systems, 2015, 2873–82.
11. Rutter M. Psychosocial resilience and protective mechanisms. *Am J Orthopsychiatry* 1987;**57**:316–31.

12. Werner E, Smith RS. The children of Kauai: a longitudinal study from the prenatal period to age ten. *J Marriage Fam* 1973;**35**:358.
13. Werner EE, Smith RS. *Overcoming the Odds: High Risk Children from Birth to Adulthood*. Cornell University Press: Ithaca, New York, United States, 1992.
14. Bennett JB, Aden CA, Broome K. *et al.* Team resilience for young restaurant workers: research-to-practice adaptation and assessment. *J Occup Health Psychol* 2010;**15**:223.
15. Patterson JM. Integrating family resilience and family stress theory. *J Marriage Fam* 2002;**64**:349–60.
16. Patterson JM. Understanding family resilience. *J Clin Psychol* 2002;**58**:233–46.
17. Walsh F. Beliefs, spirituality, and transcendence: keys to family resilience. In: McGoldrick M, Giordano J, Garcia-Preto N (eds.), *Re-visioning Family Therapy: Race, Culture, and Gender in Clinical Practice*. 2nd ed. New York: Guilford Press, 1998, 62–89.
18. Walsh F. Family resilience: a framework for clinical practice. *Fam Process* 2003;**42**:1–18.
19. Morgan PBC, Fletcher D, Sarkar M. Recent developments in team resilience research in elite sport. *Curr Opin Psychol* 2017;**16**:159–64.
20. Morgan PBC, Fletcher D, Sarkar M. Defining and characterizing team resilience in elite sport. *Psychol Sport Exerc* 2013;**14**:549–59.
21. Pangallo A, Zibarras L, Lewis R. Resilience through the lens of interactionism: a systematic review. *Psychol Assess* 2015;**27**:1–20.
22. Ayyagari R, Grover V, Purvis R. Technostress: technological antecedents and implications. *MIS Q* 2011;**35**:831–58.
23. Tarafdar M, Tu Q, Ragu-Nathan BS. The impact of technostress on role stress and productivity. *J Manag Inf Syst* 2007;**24**:301–28.
24. Connor KM, Davidson JRT. Development of a new resilience scale: the Connor–Davidson Resilience Scale (CD-RISC). *Depress Anxiety* 2003;**18**:76–82.
25. Cederblad M. Fifty years of epidemiologic studies in child and adolescent psychiatry in Sweden. *Nord J Psychiatry* 1996;**50**:3–14.
26. Carver CS, Scheier MF, Weintraub JK. Assessing coping strategies: a theoretically based approach. *J Pers Soc Psychol* 1989;**56**:267–83.
27. Hollnagel E. Resilience—the challenge of the unstable. In: Hollnagel E (ed.), *Resilience Engineering: Concepts and Precepts*. Aldershot: Ashgate Publishing Ltd. 2012, 9–18.
28. Bandura A. *Self-Efficacy: The Exercise of Control*. New York, USA: W H Freeman/Times Books/Henry Holt & Co. 1997.
29. Bandura A. Self-efficacy: toward a unifying theory of behavioral change. *Psychol Rev* 1977;**84**:191–215.
30. Bandura A. Self-efficacy mechanism in human agency. *Am Psychol* 1982;**37**:122–47.
31. Hjemdal O, Aune T, Reinfjell T. *et al.* Resilience as a predictor of depressive symptoms: a correlational study with young adolescents. *Clin Child Psychol Psychiatry* 2007;**12**:91–104.
32. Wagnild GM, Young HM. Development and psychometric evaluation of the Resilience Scale. *J Nurs Meas* 1993;**1**:165–78.
33. Windle G, Markland DA, Woods RT. Examination of a theoretical model of psychological resilience in older age. *Aging Ment Health* 2008;**12**:285–92.
34. Li L, Xu L, He W. The effects of antecedents and mediating factors on cybersecurity protection behavior. *Comput Hum Behav Rep* 2022;**5**:100165.
35. Rutter M. Resilience: some conceptual considerations. *J Adolesc Health* 1993;**14**:626–31.
36. Cederblad M, Dahlin L, Hagnell O. *et al.* Salutogenic childhood factors reported by middle-aged individuals: follow-up of the children from the Lundby Study grown up in families experiencing three or more childhood psychiatric risk factors. *Eur Arch Psychiatry Clin Neurosci* 1994;**244**:1–11.
37. Howard MC. Creation of a computer self-efficacy measure: analysis of internal consistency, psychometric properties, and validity. *Cyberpsychol Behav Soc Netw* 2014;**17**:677–81.
38. Sulimani-Aidan Y. Future expectations as a source of resilience among young people leaving care. *Br J Soc Work* 2017;**47**:1111–27.
39. Verkijika SF. 'If you know what to do, will you take action to avoid mobile phishing attacks': self-efficacy, anticipated regret, and gender. *Comput Hum Behav* 2019;**101**:286–96.
40. Fredrickson BL, Branigan C. Positive emotions broaden the scope of attention and thought-action repertoires. *Cogn Emot* 2005;**19**:313–32.
41. Duckworth AL, Quinn PD. Development and validation of the short grit scale (Grit-S). *J Pers Assess* 2009;**91**:166–74.
42. Ryan L, Caltabiano ML. Development of a new resilience scale: the Resilience in Midlife Scale (RIM Scale). *Asian Soc Sci* 2009;**5**:39–51.
43. Heiman T. Parents of children with disabilities: resilience, coping, and future expectations. *J Dev Phys Disabil* 2002;**14**:159–71.
44. Nicholson J, Coventry L, Briggs P. 'If it's important it will be a headline' cybersecurity information seeking in older adults. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019, 1–11.
45. Costello AB, Osborne J. Best practices in exploratory factor analysis: four recommendations for getting the most from your analysis. *Pract Assess Res Eval* 2005;**10**:7.
46. Fabrigar LR, Wegener DT, MacCallum RC. *et al.* Evaluating the use of exploratory factor analysis in psychological research. *Psychol Methods* 1999;**4**:272.
47. Finch H. Comparison of the performance of varimax and promax rotations: factor structure recovery for dichotomous items. *J Educ Meas* 2006;**43**:39–52.
48. Kaiser H. An index of factorial simplicity. *Psychometrika* 1974;**39**:1–6.
49. Thurstone LL. *Multiple-factor Analysis; A Development and Expansion of the Vectors of Mind*. Chicago, USA: University of Chicago Press, 1947.
50. Netemeyer RG, Boles JS, McMurrian R. Development and validation of work–family conflict and family–work conflict scales. *J Appl Psychol* 1996;**81**:400.
51. Smith BW, Dalen J, Wiggins K. *et al.* The brief resilience scale: assessing the ability to bounce back. *Int J Behav Med* 2008;**15**:194–200.
52. Harvey MR, Liang B, Harney PA. *et al.* A multidimensional approach to the assessment of trauma impact, recovery and resiliency: initial psychometric findings. *J Aggress Maltreat Trauma* 2003;**6**:87–109.
53. Kott A, Linkov I. To improve cyber resilience, measure it. *Computer* 2021;**54**:80–5.
54. Van Bavel R, Rodríguez-Priego N, Vila J. *et al.* Using protection motivation theory in the design of nudges to improve online security behavior. *Int J Hum Comput Stud* 2019;**123**:29–39.
55. Alshaikh M. Developing cybersecurity culture to influence employee behavior: a practice perspective. *Comput Secur* 2020;**98**:102003.
56. Nicholson J, Morrison B, Dixon M. *et al.* Training and embedding cybersecurity guardians in older communities. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021, 1–15.
57. Nicholson J., McGlasson J. CyberGuardians: improving community cyber resilience through embedded peer-to-peer support. In: DIS 2020 Companion—Companion Publication of the 2020 ACM Designing Interactive Systems Conference, 2020, 117–21.
58. Vakhitova ZI, Go A, Alston-Knox CL. Guardians against cyber abuse: who are they and why do they intervene? *Am J Crim Justice* 2023;**48**:96–122.
59. Morrison B, Coventry L, Briggs P. How do older adults feel about engaging with cyber-security? *Human Behav Emerg Technol* 2021;**3**:1033–49.
60. Van Steen T, Norris E, Atha K. *et al.* What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *J Cybersecur* 2020;**6**:tyaa019.
61. Zhang XA, Borden J. How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *J Risk Res* 2020;**23**:1336–52.