Human Individual Difference Predictors in Cyber-Security: Exploring an Alternative Scale Method and Data Resolution to Modelling Cyber Secure Behavior

George Raywood-Burke[1,2], Laura M. Bishop[1,2], Phoebe M. Asquith[1,2], and Phillip L. Morgan[1,2]

[1]Human Factors Excellence Research Group, School of Psychology, Cardiff University,
Tower Building, 70 Park Place, Cardiff CF10 3AT, UK
{raywood-burkeg,bishoplm2,asquithpm, morganphil}@cardiff.ac.uk
2 Airbus Central R&T, The Quadrant, Celtic Springs Business Park, Newport NP10 8FZ, UK
{george.raywood-burke.external,laura.l.bishop.external,
phoebe.p.asquith.external,phillip.morgan.external}@airbus.com

Abstract. With the increase in reliance upon technology in our everyday lives, users are more vulnerable than ever to cybercrime and data security breaches. Whilst it is important, and valued, to develop technology-based interventions to mitigate this risk, it is also important to consider the impact of human error on cyber safety, and how this can be measured. Data collected from a diverse sample of 189 participants using an alternative measurement scale to more traditional Likert scales, the Visual Analogue Scales (VAS), was adopted for previously researched measures of individual differences (Age, gender, education level, personality, decision-making style, risk-taking preferences, acceptance of the internet, and related Theory of Planned Behavior and Protection-Motivation Theory concepts) to expand understanding of the relationships between individual differences and user-end cybersecurity behaviors, and explore the significance of this alternative measure in the field of Cyber Psychology. Findings demonstrate the use of VAS can be a reliable and valid method capable of identifying a variety of potential human vulnerabilities and strengths on an individual level. These findings highlight the importance of considering a human-centered approach to cyber-security, and future research should consider then importance of these individual differences in tailoring practical interventions.

Keywords: Cyber-security behavior – Individual differences – Visual Analogue Scale

1 Introduction

Within the field of Cyber Psychology, some significant of research has focused upon technological interventions to reduce to the risk of cyber-attack [1]. Whilst technological interventions can be useful, given the advance in technology over recent years [2,3], it is also important to consider the role of the human user in preventing cyber-attacks. A recent report by CybSafe, for example, found that 90% of cyber incidents in 2019 within businesses had human error as a contributing factor [4]. Human error can

arise through system misconfiguration, poor patch management, use of default usernames and passwords/easy-to-guess passwords, lost hardware, and disclosure of regulated information via the use of incorrect email addresses [5]. Multiple cognitive elements are thought to be relevant to these behaviors and outputs, including user perception of security risk [6], company security culture and user awareness [7], intentional and unintentional maladaptive behavior [8], individual vulnerabilities and strengths [9], and contextual pressures [10].

Although research has begun to characterize the psychological aspects influencing cyber safe and cyber-risky behaviors in Human-Computer Interaction (HCI) and Human-Machine Interaction (HMI), research in this field is in its infancy. A traditional subjective measurement technique, Likert scales, appears to be the dominant scale for these forms of research – for example Bishop et al [9] has utilized 5- and 7-point Likert scales self-report measures to understand individual differences and user behavior which have provided useful insight. The aims of this present study are two-fold; first to build on knowledge regarding possible relationships between human individual differences and cyber-security behaviors. To do this, we used a self-report scale not previously used in this area - the Visual Analogue Scale (VAS). Our second aim was to evaluate reliability and validity of the VAS, compared to more widely used 5- and 7-point Likert scales. Using an alternative scale across the same measures used in Bishop et al [9], we can further our knowledge of these relationships, as well as gaining a better understanding of the extent to which different scales and measurement vectors within scales may impact findings. Using the findings from this work and drawing upon those from some other studies – such as Bishop et al [9] - we will be better able to provide recommendations to how tailored interventions could be created for practical use to aid the mitigation of human susceptibility to cyber-attacks.

2 Background

Technologically driven interventions in the field of cyber-security tend to assume a "one size fits all" solution. For example, system monitoring is a common risk mitigation driven by system anomalies, used across all users within a business. This is useful but used by in isolation does not fully address and mitigate user-centered vulnerabilities. More work research is needed on human-focused approaches – specifically to develop more targeted interventions to adapt to the ever-changing cyber-security landscape. In particular, understanding which psychological aspects of individual users may increase vulnerability to cyber-security risk is critical to further develop targeted and effective interventions.

2.1 Individual Differences in Cyber-Security

A number of studies have examined how various individual differences may relate to online cyber-security behaviors to estimate human cyber-security strengths and vulnerabilities, for example the SeBIS Online Security Behaviors Questionnaire [11]. This framework, and others, are based upon well-researched psychological models of predicting behavior, attitudes, and intentions including the Protection Motivation Theory [12] and the Theory of Planned Behavior [13]. Using these methods gender has been found to be a significant predictor of some cyber secure behaviors - whereby men may be more likely to form stronger passwords, engage in updating software more regularly,

and search for cyber risk cues proactively [14]. Some aspects of personality such as conscientiousness may also predict select cyber secure behaviors [14-16]; and risk-taking attitude, decision making strategies and impulsivity have also been found to be significantly related to cyber secure behaviors [11].

More recently, attempts have been made to refine individual difference models of cyber secure behavior, as some measures are highly correlated across frameworks [11,17,18]. The present study work aims to calculate the significance of a range of independent individual difference measures in predicting cyber secure behavior. However, there are noted differences in findings that need to be addressed. For example - Gratian et al [14] found gender predicted cyber secure behavior, and higher impulsivity has been found to be significantly negatively correlated to cyber secure behaviors [11]. However, these significant findings were not found in Bishop et al [9].

2.2 Measurement Techniques and Data Resolution

Whilst there is a possibility that discrepancies in findings on gender and impulsivity could be due to co-variance of predictors or indeed low power, it is also important to critique the method of self-report and the potential influencing role on findings. In Egelman and Peer [11] and Bishop et al [9], participants rated items on either 5- or 7-point Likert scales (ordinal data). In these instances, each point is essentially a 'landmark' on a scale – e.g. an extreme value at each end of the scale, a neutral value in the middle, and equally distanced points / gradations leaning to one extreme or another (see Figure 1, left). Whilst Likert scales like these have the benefit of demonstrating the direction an individual may agree or disagree with presented statements (unless a neutral rating is selected), the degree of rating extremity comparison in variability between participants is less clear as there are only a few points to choose from on the scale – e.g., '1', '2', '4,' or '5' on a five-point scale. Furthermore, these points are fixed in equal points away from each other; thus, individuals could be more likely to form a central tendency (e.g. gravitate towards a neutral rating) or be polarized in the direction of one 'landmark' or the other. Having a number of differing points for different Likert scale predictors for individual differences in the same model also serves as a problem - data for those with more points can be viewed to a greater resolution, impacting the significance (or not) of analyses used.

A solution that potentially addresses all of these issues is proposed and presented in the current paper. The proposed method is to use scales collecting data closer to interval rather than ordinal properties, to increase the freedom of choice in selecting *an area*, rather than fixed data-point on the scale. Whilst Wu and Lueng [19] conclude data distribution is easier to interpret when there is an increase to 11-points on Likert scales as data is closer to that of interval data (e.g., '1' similar to 10% agree, '10' similar to 100% agree) there could still be the issue of fixed 'landmark' points polarizing ratings. This problem, however, is arguably mitigated in Visual Analogue Scales (VAS) – whereby the only fixed ratings on a scale are those at the polar ends (0 and 100), with a continuous line between them (See Figure 1, right). Participants simply mark a point on the continuous line without being polarized by landmarks and resulting data would approximate an interval-scale level [20] through measurement of points marked – e.g., on a scale of 0-100 or even at a finer grained level – e.g., with decimal places.

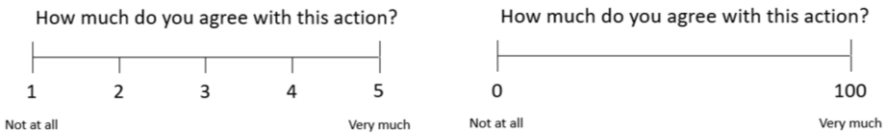

Figure 1 – Example of a 5-point Likert scale (left) and a Visual Analogue Scale (right).

With these things in mind, this paper explores whether the use of VAS in human cyber-security strength and vulnerability measures is suitable to form models investigating relationships between individual differences (gender, age, education, personality, risk-taking, decision-making, impulsivity, acceptance of the internet, and relevant Theory of Planned Behavior and Protection-Motivation Theory concepts) and cyber secure behaviors (device securement, updating, password generation, and proactive awareness), how this compares to findings collected using more commonly used Likert scales, predicting similar findings to those found in Bishop et al [9], and to note what could be gained from adopting these measures.

3 Method

3.1 Participants

189 participants (109 Male, 79 Female, 1 Non-Binary) with a good level of the English Language and normal/corrected-to-normal vision were recruited voluntarily via Prolific online marketing tool [21]. Participants were aged between 18 and 56 years old (M = 24.53, SD = 6.40), and were well educated (all educated at least up to UK GCSE), with 90% holding at least UK A level or equivalent qualifications, and 58.3% holding at least an undergraduate degree. Informed consent was obtained from all participants and upon completion all were fully debriefed and were compensated £7.50 for participation. This study was approved by Cardiff University School of Psychology Research Ethics Committee (CU-SREC).

3.2 Study Design, Materials and Procedure

Using a between-subjects design, this study investigated how individual differences (gender, age, education, personality, risk-taking, decision-making, impulsivity, acceptance of the internet) and component factors within both Protection-Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) related to cyber-security behaviors (See Table 1 for summary of subscale measures).

Participants signed up to the study on Prolific [21] and accessed the survey tool via a link from their laptop or desktop PCs. The survey was created on Qualtrics©, an online survey platform. Upon reading a brief introduction sheet and consenting to take part in the study, participants were first asked to provide their demographic information including age, education level, and gender, before completing measures for individual differences and cyber secure behavior. The first measure was the SeBIS online security behavior questionnaire [11] consisting of 16 statements containing items made up of four subscales (updating, device securement, password generation, and proactive

awareness). Participants provided ratings for each statement on a VAS, reflecting how often they exhibit these behaviors (0=Never, 100=Always).

Personality IPIP traits [15] consisted of 50 statements (10 each relating to subscales including Extraversion, Openness, Conscientiousness, Neuroticism, and Agreeableness). Participants were asked to rate the extent to which each statement applied to themselves on a VAS (0=Completely disagree, 100=Completely agree). For the Decision-making GDMS questionnaire [22] participants were asked to rate the extent to which they agree/disagree with 25 statements, representing five decision-making styles (five each for intuitive, dependent, avoidant, rational, spontaneous style) on a VAS (0=Completely disagree, 100=Completely agree).

Participants were asked to rate how likely they were to engage in 30 risky behaviors from the DOSPERT Risk-taking preferences [23] on a VAS (0=Never, 100=Definitely). These 30 items were subdivided into subscales each containing six questions per subscale (social, recreational, financial, health/safety, ethical).

For impulsivity, participants gave ratings on the Barrett Impulsiveness Scale (BIS-11) [24] to indicate how regularly they had experienced a list of 30 statements, on a VAS ranging from 0 (Completely disagree) to 100 (Completely agree). Next, the UTAUT2 was used to assess the acceptance of the internet [25]. This questionnaire consists of 30 statements with nine subscales (performance expectancy, effort expectancy, social influence, trust, facilitating conditions, hedonic motivation, price value, habit, and behavioral intention), rating the extent to which the participant agrees with each statement on a VAS (0=Completely disagree, 100= Completely agree).

Finally, a combined list of 43 statements relating to cyber behaviors and the PMT and TPB [17] was presented. This formed nine subscales (Information security awareness, information security organization policy, information security experience and involvement, attitude, subjective norms, perceived behavioral control, threat appraisal, information security self-efficacy, information security conscious care behavior), each with a VAS to rate the extent to which they agree with statements presented (0=Completely disagree, 100=Completely agree). Before exiting the survey platform, participants were then provided with debrief information and provided with a Prolific code for participation payment.

Attention check items (e.g. To ensure you are paying attention please rate this as 0) were randomly placed across all measures to test whether attention to items was maintained throughout, and all checks were met for all participants. All items within each measure were randomized in order to reduce inattentive ratings for similar items.

Table 1. Summary of subscales for individual differences and cyber secure behavior measures.

Measurement	Subscales
Demographics	Age Group (18-24, 25-34, 35-44, 45-54, 55-64) Gender Education level (GCSEs or Equivalent, A-levels or Equivalent, Undergraduate degree, Masters degree, PhD/Doctorate, Other specified)
IPIP Personality [15]	Extraversion Openness Conscientiousness Neuroticism Agreeableness
GDMS Decision-making style [22]	Intuitive Dependent Avoidant Rational Spontaneous
DOSPERT Risk-taking preferences [23] (Likelihood of engaging in risky behaviours scales only)	Social behavior Recreational behavior Financial behavior Health/Safety behavior Ethical behavior
Barratt Impulsiveness Scale [24]	BIS-11 Total
UTAUT2 Acceptance of the Internet [25]	Performance expectancy Effort expectancy Social influence Trust Facilitating conditions Hedonic motivation Price value Habit Behavioral intention
Combined PMT and TPB Questionnaire [17]	Information security awareness Information security organisation policy Information security experience and involvement Attitude Subjective norms Perceived behavioral control Threat appraisal Information security self-efficacy Information security conscious care behavior
SeBIS online security behaviour [11]	Updating Device securement Password generation Proactive awareness

4 Results

We are interested in exploring relationships between demographic categories (age, gender, and education level) and individual differences (personality, risk-taking, decision-making, impulsivity, acceptance of the internet, and relevant Theory of Planned Behavior and Protection-Motivation Theory concepts), with a variety of cyber security behaviors (Updating, device securement, Password generation, and Proactive awareness). Results are grouped according to the 4 subscales from the SeBIS online behaviors questionnaire [11]: device securement (section 4.1) proactive awareness (section 4.2), updating (section 4.3) and password generation (section 4.4). VAS scale ratings were classified as ordinal and therefore non-parametric statistical tests were used. Table 2 provides an overall summary of findings and how they compare to Bishop et al. [9].

Independent-samples Kruskal-Wallis (K-W) tests compared responses from each of 4 SeBIS subscales across demographic groups age, gender, and education levels. Spearman's rank 2-tailed correlations compared responses from each of the 4 SeBIS subscales with subscales from individual differences questionnaires. These were self-reported personality traits [15], Decision-making styles [22], Risk-taking preferences [23], Impulsivity [24], Acceptance of the Internet [25], and other cyber behavior statements developed in accordance with PMT and TPB [17].

Mean substitution imputation was used in cases where data was missing for individual item measures to reduce bias. Cronbach's Alpha test was used to test internal consistency between subscale items for all questionnaire measures**.** Internal consistency at $\alpha > 0.5$ was found for all subscales except for Introversion component of the IPIP Extraversion subscale ($\alpha = .425$) and Facilitating conditions subscale of the UTAUAT2 ($\alpha = .164$).

4.1 SeBIS Device Securement

An independent-samples K-W test revealed no significant differences between age groups, gender or education levels on the SeBIS device securement subscale. Neuroticism was found to a significant weak negative correlation with the SeBIS Device Securement subscale ($r = -.161$, $n = 189$, $p = .027$) but no significant relationships were found for other personality subscales.

Ethical and Avoidant decision-making styles both had significant but weak negative correlations with Device Securement ($r = -.162$, $n = 189$, $p = .026$ and $r = -.147$, $n = 189$, $p = .044$ respectively). Rational decision-making style had a significant weak positive correlation with Device Securement ($r = .159$, $n = 189$, $p = .029$). There were no significant relationships found for Intuitive and Spontaneous GDMS subscales and Device Securement. No significant relationships were found between any DOSPERT subscales and Device Securement.

A significant weak negative relationship was found between Impulsivity and Device Securement ($r = -.144$, $n = 189$, $p = .048$). No significant correlations were found for any UTAUT2 subscales and Device Securement.

Analysis found there were significant positive correlations between Device Securement and Information Security Awareness ($r = .293$, $n = 189$, $p < .001$), Information Security Organization Policy ($r = .170$, $n = 189$, $p = .019$), Information Security Experience and Involvement ($r = .259$, $n = 189$, $p < .001$), Attitude ($r = .264$, $n = 189$, $p < .001$), Perceived Behavioral Control ($r = .202$, $n = 189$, $p = .005$), Threat Appraisal ($r = .213$, $n = 189$, $p = .003$), and Information Security Conscious Care Behavior ($r = .270$,

n = 189, p < .001). No significant correlations were found between Device Securement and Subjective Norms or Information Security Self-Efficacy subscales from the combined PMT/TPB questionnaire.

4.2 SeBIS Proactive Awareness

Using a K-W test, no significant differences were found between age, gender, or education levels with the SeBIS Proactive Awareness subscale. For the IPIP personality subscales, significant positive correlations were found between Proactive Awareness and Agreeableness (r = .196, n = 189, p = .007), Conscientiousness (r = .221, n = 189, p = .002), and Openness (r = .258, n = 189, p < .001). No other significant findings were found for other personality subscales and Proactive Awareness. For the GDMS decision-making subscales, Proactive Awareness ratings were found to have significant negative correlations with Intuitive (r = -.181, n = 189, p = .013), Avoidant (r = -.156, n = 189, p = .032), and Spontaneous subscales (r = -.218, n = 189, p = .003). A significant positive correlation as found between Proactive Awareness and the Rational GDMS subscale (r = .282, n = 189, p < .001), however no significant correlation was found between Proactive Awareness and the Ethical GDMS subscale. For Proactive Awareness ratings and DOSPERT risk-taking subscales, Proactive Awareness was found to significantly correlated in a negative relationship with only the Recreational Behavior subscale (r = -.198, n = 189, p = .006) and Ethical Behavior (r = -.272, n = 189, p < .001).

Impulsivity was found to be significantly negatively correlated with Proactive Awareness (r = -.352, n = 189, p < .001). For Acceptance of the Internet subscales and Proactive Awareness, Performance Expectancy (r = .168, n = 189, p = .021) and Effort Expectancy (r = .163, n = 189, p = .025) scales positive correlated with Proactive Awareness but negatively for Trust (r = -.150, n = 189, p = .039).

Analysis of the subscales from the combined PMT and TPB questionnaire found there were significant positive correlations between Proactive Awareness and Information Security Awareness (r = .316, n = 189, p < .001), Information Security Organization Policy (r = .288, n = 189, p = .001), Information Security Experience and Involvement (r = .278, n = 189, p < .001), Attitude (r = .311, n = 189, p < .001), Perceived Behavioral Control (r = .172, n = 189, p = .018), Threat Appraisal (r = .299, n = 189, p < .001), Information Security Self-Efficacy (r = .219, n = 189, p = .002), and Information Security Conscious Care Behavior (r = .309, n = 189, p < .001). No significant correlations were found between Proactive Awareness and the Subjective Norms subscale from the combined PMT/TPB questionnaire.

4.3 SeBIS Updating

No significant differences were found between age, gender, or education levels and Updating SeBIS subscale ratings using a K-W test. For Personality, a significant finding was only found for the Openness subscale and Updating showing a positive correlation (r = .211, n = 189, p = .004). For GDMS decision-making subscales, Avoidant style ratings were significantly negatively correlated to Updating (r = -.151, n = 189, p = .038) and Rational style ratings were significantly positively correlated to Updating ratings (r = .238, n = 189, p < .001). No other GDMS subscales significantly correlated with Updating. Regarding the DOSPERT questionnaire, only the Ethical Behavior

subscale was significantly correlated with Updating demonstrating a weak negative relationship ($r = -.193$, $n = 189$, $p = .008$).

Impulsivity was found to have a significant negative relationship with Updating ($r = -.250$, $n = 189$, $p = .001$). Of the Acceptance of the Internet subscales, only Performance Expectancy and Hedonic Motivation demonstrating significant findings revealing weak positive correlations with Updating ($r = .151$, $n = 189$, $p = .038$ and $r = .161$, $n = 189$, $p = .027$ respectively).

Analysis of the subscales from the combined PMT and TPB questionnaire found there were significant positive correlations between Updating and Information Security Awareness ($r = .324$, $n = 189$, $p < .001$), Information Security Organization Policy ($r = .317$, $n = 189$, $p < .001$), Information Security Experience and Involvement ($r = .249$, $n = 189$, $p = .001$), Attitude ($r = .228$, $n = 189$, $p = .002$), Perceived Behavioral Control ($r = .174$, $n = 189$, $p = .016$), Threat Appraisal ($r = .216$, $n = 189$, $p = .003$), Information Security Self-Efficacy ($r = .179$, $n = 189$, $p = .014$), and Information Security Conscious Care Behavior ($r = .296$, $n = 189$, $p < .001$). No significant correlations were found between Updating and the Subjective Norms subscale from the combined PMT/TPB questionnaire.

4.4 SeBIS Password Generation

From the use of an independent-sample K-W test, it was found there was no significant difference found between gender, age groups, or education levels for the SeBIS Password Generation subscale. For personality, Password Generation was found to significantly positively correlated with Conscientiousness ($r = .229$, $n = 189$, $p = .002$) and Openness ($r = .147$, $n = 189$, $p = .043$) subscales only. Regarding decision-making, Password Generation was significantly negatively correlated with Avoidant decision-making style ratings ($r = -206$, $n = 189$, $p = .005$) and significantly positively correlated with Rational style ratings ($r = .167$, $n = 189$, $p = .021$), but other subscales yielded non-significant results. No significant relationships were found between Risk-taking preference subscales and Password Generation.

Impulsivity was found to have a significant negative correlation with Password Generation ($r = -.219$, $n = 189$, $p = .002$). Only Trust ($r = -.153$, $n = 189$, $p = .036$) and Habit ($r = -.192$, $n = 189$, $p = .008$) subscales of the Acceptance of the Internet measures were found to significantly correlate with Password Generation, demonstrating a negative relationship.

Analysis of the subscales from the combined PMT and TPB questionnaire found there were significant positive correlations between Updating and Information Security Awareness ($r = .302$, $n = 189$, $p < .001$), Information Security Organization Policy ($r = .240$, $n = 189$, $p = .001$), Information Security Experience and Involvement ($r = .266$, $n = 189$, $p < .001$), Attitude ($r = .276$, $n = 189$, $p < .001$), Perceived Behavioral Control ($r = .188$, $n = 189$, $p = .010$), Threat Appraisal ($r = .236$, $n = 189$, $p = .001$), Information Security Self-Efficacy ($r = .191$, $n = 189$, $p = .008$), and Information Security Conscious Care Behavior ($r = .277$, $n = 189$, $p < .001$). No significant correlations were found between Updating and the Subjective Norms subscale from the combined PMT/TPB questionnaire.

Table 2. Findings from correlational analyses of individual difference subscales and the SeBIS online security behavior subscales. *Note. 1=Positive relationship, 2=Negative relationship, - represents no significant relationship, a = Significant finding consistent with Bishop et al.* [9]

Individual difference	Device securement	Proactive awareness	Updating	Password generation
Demographics	-	-	-	-
Personality	Neuroticism[2]	Agreeableness[1] Conscientiousness[1] Openness[1]	Openness[1]	Conscientiousness[1] Openness[1]
Decision-making	Ethical[2] Avoidant[2] Rational[1]	Intuitive[2] Avoidant[2] Rational[1] Spontaneous[2]	Avoidant[2] Rational[1]	Avoidant[2 a] Rational[1]
Risk-taking	-	Recreational behavior[2] Ethical behavior[2]	Ethical behavior[2]	-
Impulsivity	BIS-11 Total[2]	BIS-11 Total[2]	BIS-11 Total[2]	BIS-11 Total[2]
Acceptance of the Internet	-	Performance expectancy[1] Effort expectancy[1 a] Trust[2 a]	Performance expectancy[1] Hedonic motivation[1 a]	Trust[2] Habit[2]
PMT & TPB	ISA[1] ISOP[1 a] ISEI [1] Attitude[1 a] PBC[1] Threat appraisal[1 a] ISCCB[1]	ISA[1 a] ISOP[1 a] ISEI[1 a] Attitude[1 a] PBC[1 a] Threat appraisal[1 a] ISSe[1 a] ISCCB[1]	ISA[1 a] ISOP[1 a] ISEI[1 a] Attitude[1 a] PBC[1] Threat appraisal[1 a] ISSe[1 a] ISCCB[1]	ISA[1 a] ISOP[1] ISEI[1] Attitude[1 a] PBC[1 a] Threat appraisal[1 a] ISSe[1] ISCCB[1]

Note. ISA = Information Security Awareness, ISOP = Information Security Organization policy, ISEI = Information Security Experience and Involvement, PBC = Perceived Behavioral Control, ISSe = Information Security Self-efficacy, ISCCB = Information Security Conscious Care Behavior.

5 Discussion

This study set out to investigate how various individual difference (gender, age, education, personality, risk-taking, decision-making, impulsivity, acceptance of the internet, and relevant Theory of Planned Behavior and Protection-Motivation Theory concepts) measures may impact a variety of cybersecurity behaviors (updating, device securement, password generation, and proactive awareness). Findings found a number of significant findings, primarily combined TPB and PMT concepts (See Table 2), that support Bishop et al [9]. Significant, and consistent, findings were also found notably for measures of personality, decision-making style, risk-taking preferences, impulsivity, and select measures of Acceptance of the Internet. However, a some of these results from using Visual Analogue Scales show deviance from previous research and are discussed below. The findings from this study not only convey the importance of considering end-user strengths and vulnerabilities to mitigate the risks of cyber-attacks, but also suggest the use of Visual Analogue Scales for these measures are reliable and valid.

The first dimensions of individual differences investigated in the present study were age, gender, and level of education to examine whether demographically participants differed in engagement with various online security behaviors. Whilst Gratian et al [14] had found that men were significantly more likely to engage in a range of good cyber secure behaviors compared to women, like Bishop et al [9], we found no significant differences between groups for gender – despite having a balanced sample. Similarly, we also found no differences between age groups or levels of education. However, Gratian et al [14] employed a larger sample and their results show the significant gender differences are very weak relationships, thus findings could differ due to this sample difference.

Regarding personality, unlike Bishop et al [9] which found no significant relationships for any subscales, we found conscientiousness to have a significant positive relationship with Proactive Awareness – a consistent finding with Gratian et al [14] to a similar degree of effect size. However, in the present study we found no significant relationship between extraversion and device securement – differing from some previous research on perceived security risks [14,26]. Although, significant findings were also found for conscientious and password generation, and higher openness being related to higher password generation and proactive awareness. This significant finding across more than one form of cyber secure behavior could signify how select individual differences may be more significant to reducing cyber-security risks from an end-user perspective compared to others. This remains true when examining decision-making styles and observing consistent positive relationships for rational styles across all cyber secure behaviors measured, and how avoidant styles of decision-making should be (ironically) avoided due to their negative relationship across all SeBIS behaviors – although further analysis is needed to further understand the nature of these relationships.

Furthermore, findings found less ethical, riskier, behavior was significantly negatively related to updating and proactive awareness could indicate the need for libertarian paternalism, or ‘nudges’ [27,28]. However, as no significant relationship was found for password generation or device securement it is not clear whether these forms of nudges would be effective for these cyber secure behaviors. However, it is of interest to understand how these forms of interventions could be adapted to reduce impulsivity – as

ratings for this measure found to be a significantly related to all measured forms of cyber secure behaviors. Regarding participants' acceptance of the internet, the degree of trust individuals has in relation to password generation and likelihood of engaging in proactive awareness appears to be of interest as this could highlight a particular significant vulnerability which cyber offenders could take advantage of using targeted persuasion techniques.

For a large number of subscale measures from the combined PMT/TPB questionnaire [17] it is encouraging to see consistent findings with previous research [9] as this could suggests not only that these individual differences be reliably measured, but that VAS are capable of detected similar findings. A potential reason for these findings being found to be significant in both Bishop et al [9] and the present study, but not measures in personality, decision-making styles, or impulsivity, could be in part due to the differences in participant sizes and the strength of relationships found. On average, significant correlations found from the PMT/TPB questionnaire appear to be stronger than a number of other relationships found – suggesting the variance of behavior accounted for could be greater in relation to motivation and planned behavior. However, this needs further analysis to determine precisely. The present study also furthers Bishop et al [9] due to the greater diversity in the sample data is collected. By collecting data from participants from a mixture of mainly European and American countries, we can be more confident findings being applicable to the general population and across cultures. To further validate this, further investigations should adopt the VAS in subjective measurements to evaluate replicability in diverse samples.

6 Limitations

As with these forms of online survey studies, not all responses may truly represent participants' ratings for individual difference and cyber secure behavior measures – therefore the true extent to which these ratings represent individuals may be open to responder biases. However, attention checks and data quality checks were carried out to reduce the likelihood of attention significantly influencing overall data analyses, and all items were randomized within each measure to reduce the likelihood of inattentive responses.

As correlational analyses were mainly used between variables, it cannot be concluded at this stage the nature of these variables and the extent to which individual differences variance may account for cyber secure behaviors. Although further analysis to form regression models with other potential individual difference predictors will be explored to evaluate how interventions for cyber risk could be best targeted in varying contexts. Whilst the present study does indicate the use of Visual Analogue Scales could be a valid alternative for exploring relationships between variables, it cannot at this stage be determined whether this form of scale may be more beneficial than traditional Likert scales. A comparison between the use of VAS and Likert scales for variables using data from similarly derived sources whilst controlling for sample size should be a future direction in this field to determine how measurement of the same data in different forms may influence the distributions and significance of data.

It was noted from the use of Cronbach's Alpha tests a few scales appeared to have questionable or weak internal consistency. Facilitating conditions subscale of the UTAUAT2 (α = .164) and the IPIP introversion sub-component of the Extraversion

subscale (α = .425) in particular had very low consistency, which in turn may limit the extent to which these specific findings in relation to cyber secure behavior measurements may be debatable and need further exploration to examine whether specific items may limit these analyses. It was also noted internal consistency for the disagreeable sub-component of the IPIP Agreeableness subscale (α = .55) and Performance Expectancy subscale of the Acceptance of the Internet questionnaire were close to the moderate internal consistency threshold, suggesting the degree these specific measures are measuring their overarching concept needs to be explored further. Finally, as only moderate internal consistency was found for Updating and Device Securement subscales from the SeBIS questionnaire (α = .524 and α = .523 respectively), with Proactive Awareness and Password Generation SeBIS subscales close to the upper end of the moderate threshold (α = .598 and α = 601 respectively), there is a necessity to explore whether specific items may influence significance of relationships.

7 Conclusions and Future Directions

Considering currently how increasingly reliant people are on technology for both work and leisure, it is also of paramount importance to consider how valued users are to mitigate the rising threat of cyber-security breaches and incidents. As highlighted from the results from this study, both vulnerabilities and strengths of individuals need to be truly understood with the aim for these to be utilized in the tailoring of interventions at both individual and organizational levels. Understanding the extent to which user variables relate to security behaviors is the next logical step to determine how humans can become the strongest defense to online risks. The findings from this study not only convey the importance of considering end-user strengths and vulnerabilities to mitigate the risks of cyber-attacks, but also suggest the use of Visual Analogue Scales for these measures are reliable and valid. Future research using more direct comparisons of Likert and VAS data should be carried out to evaluate the extent to which these measurement scales alter data resolution and distribution. From an increase in data resolution, this could allow for finer adjustment to Human-Computer Interaction (HCI) and Human-Machine Interaction (HMI) measurements and interventions - For example, accurately understanding how different people are likely to secure personal and work devices, how perceptions of cyber-security policy influence likelihood in ensuring software is updated, how actively individuals may seek to keep up-to-date with ever-changing cyber-security risks, and trust of equipment used can we fine-tune efficient interventions. There is a need to consider the interactions between individuals and the environment in which they sit to fully comprehend which behaviors can be, and should be, encouraged or avoided; and when hard constraints built into HMI and HCI designs may be more appropriate in a way which does not hinder productivity or increase harm.

Acknowledgements. This research was supported through an Endeavr Wales funded PhD studentship awarded to the first author (George Raywood-Burke) from the School of Psychology at Cardiff University. Other support was provided by Airbus where the PhD student is a member of the Airbus Accelerator in Human-Centric Cyber Security team, under the Technical Leadership of the fourth author (Professor Phillip Morgan) who is also George Raywood-Burke's PhD Lead Supervisor.

References

1. Singh & Silakari. (2009). A survey of cyber attack detection systems. *International journal of computer science and network security*, 9, 5, 1-10.
2. Gupta, M., Abdelsalam, M., Khorsandroo, S., and Mittal, S. (2020). Security and privacy in smart farming: Challenges and Opportunities. *IEEE Access*, 8, 34564-34584. Doi: 10.1109/ACCESS.2020.2975142.
3. Okamoto. (2015). SecondDEP: Resilient computing that prevents shellcode execution in cyber-attacks. *Procedia computer science*, 60, 691-699.
4. CybSafe. (2020). Human error to blame for 9 in 10 UK cyber data breaches in 2019. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/ . *Accessed 12.03.21*.
5. IBM Security Services. (2014). Cyber Security Intelligence Index. Accessed October 30th, 2019. http://media.scmagazine.com/documents/82/ibm_cyber_security_ intelligenc_20450.pdf.
6. Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in human behavior*, 75, 547-559.
7. Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information Security Decision Making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117-129. https://doi.org/10.1177/1555343415575152
8. Chowdhury, Adam, & Skinner. (2019). The impact of time pressure on cybersecurity behaviour: A systematic review. *Behaviour & information technology.* Doi: 10.1080/0144929X.2019.1583769
9. Bishop, L.M., Morgan, P.L., Asquith, P.M., Raywood-Burke, G., Wedgbury, A., Jones, K. (2020). Examining Human Individual Differences in Cyber Security and Possible Implications for Human-Machine Interface Design. In: Moallem A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2020. Lecture Notes in Computer Science, vol 12210. Springer, Cham.
10. Dykstra, J., & Paul, C. L. (2018). Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. In *11th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 18)*.
11. Egelman, S., & Peer, E. (2015, April). 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 (pp. 2873-2882). ACM.
12. Van Bavel, R. Rodriguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behaviours. *International journal of human computer studies*, 123, 29-39.
13. Ajzen, I. (2011). The theory of planned behaviour: reactions and reflections. *Psychological health*, 26, 9, 1103-1127.

14. Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2017). Correlating human traits and cybersecurity behaviour intentions. *Computers and security*, 73, 345-358.
15. Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, 9, 4, 475–480. https://doi.org/10.1037/ppm0000247
16. Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), 179-214.
17. Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organisations. *Computers and security*, 53, 65-78.
18. Sommestad, T. Karlzen, H., & Hallberg, J. (2015). The sufficiency of theory of planned behaviour for explaining information security policy compliance. *Security culture and information technology*, 23, 2, 200-217.
19. Wu, H., & Leung, S-O. (2017). Can Likert Scales be Treated as Interval Scales? — A Simulation Study, *Journal of Social Service Research*, 43, 4, 527-532, DOI: 10.1080/01488376.2017.1329775
20. Reips, UD., Funke, F. (2008). Interval-level measurement with visual analogue scales in Internet-based research: VAS Generator. *Behavior Research Methods*, 40, 699–704. https://doi.org/10.3758/BRM.40.3.699
21. Prolific Academic Ltd, Oxford, UK. www.prolific.co
22. Scott, S. G., & Bruce, R. A. (1995). Decision-making style: The development and assessment of a new measure. *Educational and psychological measurement*, 55(5), 818-831.Blais, A. R., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgement and decision making*, 1, 1, 33-47.
23. Blais, A. R., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgement and decision making*, 1, 1, 33-47.
24. Patton, J. H., Stanford, M. S., & Barratt, E. S. (1995). Factor structure of the Barratt impulsiveness scale. *Journal of clinical psychology*, 51, 6, 768-774.
25. Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 157- 178.
26. Riquelme, I., and Roman, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers? *Electronic markets*, 135-149.
27. Thaler, R., and Sunstein, C. (2003). Libertarian Paternalism. *The American Economic Review*, 93, 175–79.
28. Thaler, R., and Sunstein, C. (2008). Nudge: Improving decision about health, wealth, and happiness. Yale University Press.