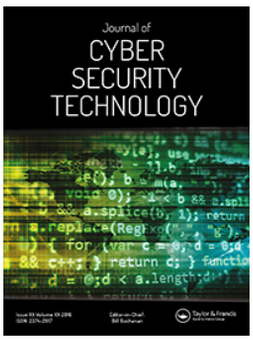

Journal of Cyber Security Technology

ISSN: 2374-2917 (Print) 2374-2925 (Online) Journal homepage: http://www.tandfonline.com/loi/tsec20

Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors

Justin D Russell, Carl F Weems, Irfan Ahmed & Golden G. Richard III

To cite this article: Justin D Russell, Carl F Weems, Irfan Ahmed & Golden G. Richard III (2017): Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors, Journal of Cyber Security Technology, DOI: 10.1080/23742917.2017.1345271

To link to this article: http://dx.doi.org/10.1080/23742917.2017.1345271

Published online: 17 Jul 2017.

JOURNAL OF CYBER SECURITY TECHNOLOGY, 2017
https://doi.org/10.1080/23742917.2017.1345271

Taylor & Francis
Taylor & Francis Group

RESEARCH ARTICLE

Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors

Justin D Russell[a], Carl F Weems[b], Irfan Ahmed[c] and Golden G. Richard III[d]

[a]Department of Psychology, Iowa State University, Ames, Iowa, USA; [b]Department of Human Development and Family Studies, Iowa State University, Ames, Iowa, USA; [c]Department of Computer Science, University of New Orleans, New Orleans, Louisiana, USA; [d]Division of Computer Science and Engineering, Louisiana State University, Louisiana, USA

ABSTRACT

The present study provides initial data on self-reported secure and insecure cyber behaviour using the iSECURE. A theoretical model for item pool development, distributions and convergent associations is presented. Data on the distribution of self-report of secure and insecure cyber behaviour is presented as well as data on factor structure of scores collected from a sample of 210 college-age adults (56.7% female). Exploratory factor analysis indicated a two-factor solution, with items loading onto subscales of secure or unsecure cyber behaviour. Comparison with an existing measure of attitudes about cyber security suggested good convergent validity. Additional analyses examined correlations between the iSECURE and Big Five personality traits as well as other personality and behavioural characteristics. The distribution of responses suggests that self-report may be useful in research studies that attempt to build towards predicting actual behaviour. The implications of findings for future research are discussed in terms of the need to develop additional techniques such as the use of real-world scenarios.

ARTICLE HISTORY
Received 8 February 2017
Accepted 19 June 2017

KEYWORDS
Cyber security; computer security; callous–unemotional traits; anxiety; Big Five; factor analysis

Introduction

Increasingly, the academic, government and business communities are calling for improved understanding of personality, behavioural and cognitive factors in cyber security [1–3]. Development of a conceptual definition (i.e. construct domain) of cyber secure\insecure behaviour is a critical first step in designing measurement and requires careful conceptual and theoretical consideration. Secure\insecure computer behaviour falls under the overarching concept of cyber security. Scholars continue to debate the criteria and behaviours necessary to define a 'cyber secure' state [4]. The federal Committee on National Security Systems provides the following brief definition of cyber secure: 'The ability to protect or defend the use of cyberspace from cyber-attacks' [5, p.22]. Cyber secure or insecure behaviour would therefore constitute actions that promote or disrupt this ability, respectively. An important next step in actualising the

CONTACT Carl F Weems cweems@iastate.edu Department of Human Development and Family Studies, Iowa State University, 4380 Palmer, 2222 Osborn Drive, Ames, IA 50011, USA

benefits of psychological research on cyber security is to empirically establish the ability to measure the dependent variable of secure and insecure behaviour.

Anderson and Agarwal [6] provide empirical support for their measures of a related concept of user *beliefs* about secure\insecure cyber behaviour. Their 'Practicing Safe Computing' (PSC) scales are a series of three, 4-item measures assessing a variety of attitudes and beliefs about computer security and the Internet, such as self-efficacy in protecting against cyber threats, attitudes about security behaviours and perceived societal norms about cyber security. Theoretically, each of these constructs may be highly related to actual security behaviours, making the PSC subscales a useful tool in establishing the construct validity of future measures assessing secure\insecure cyber behaviour.

In a review, Crossler et al. [7] caution against the use of self-report to assess unethical cyber behaviour, stating that, 'people are not generally willing to admit committing [unethical] behaviors' (p. 96). Data on this proposition is lacking. If participants are unlikely to admit to engaging in unethical cyber behaviour, the distribution of scores should show severe positive skew (i.e. the vast majority of respondents failing to endorse engaging in unethical behaviour). In this study, we examine the distributions of items consistent with the above definition of secure and insecure behaviour, utilise factor analysis to empirically identify iSECURE subscales and evaluate construct validity. We expect to find that iSECURE items tend to organise along two main factors representative of secure and insecure cyber behaviour, and that each subscale will correlate with other similar measures.

We also examine the iSECURE in terms of factor associations with the 'Big Five' traits, contributing to a developing body of work linking personality and cyber security behaviour. Research has established links between Big Five traits and compliance with security policies, susceptibility to attack and likelihood of engaging in insider attack [1,8–10]. Theoretically, conscientiousness may be a protective factor against malicious cyber behaviour, given its association with obedience [11,12].We follow from the work of McBride et al. [1] in hypothesising that neuroticism may be a predictor of a broad tendency to engage in secure cyber behaviours. Neurotic individuals may be more attentive to danger and thus more cautious in their computer use. We hypothesise that conscientiousness may also be linked to secure cyber behaviour. Conscientious individuals are more likely to abide by rules and responsibility, and accordingly should be more likely to abide by general best practices, or network policies.

There are also a number of individual differences that may predict cyber behaviour. Here we focus on anxiety, aggressive behaviour and callous–unemotional traits. Individuals with callous–unemotional traits may be more likely to commit cybercrimes such as insider attack, due to a lack of empathy for the victims or lack of personal connection to the organisation. Indeed, callousness is as a risk factor for criminal behaviour, generally [13,14]. Highly aggressive individuals may be more likely to perceive organisational injustice or personal slights, and engage in disruptive cyber behaviour as retaliation. Similarly, anxiety may play a role in user compliance in cyber-attacks. For example, anxious may be more likely to comply with social engineering attacks, given links between anxiety and susceptibility to social pressures. Drawing from the theoretical links described above, we hypothesise that these traits will be associated with higher levels of insecure behaviour.

Materials and methods

Participants

Study data were gathered from socioeconomically and ethnically diverse sample of 210 adults (56.7% female). A majority reported their ethnicity as Euro-American (51.2%), with smaller percentages identifying as African-American (15.9%), Asian-American (13.5%), Hispanic (9.1%) or another ethnic group (9.6%). Total family income was well distributed, with 22.1% reporting yearly income below $20,000, 36.1% reporting income between $20,000 and $50,000 and 36.5% reporting income above $50,000. Participants most commonly reported having between 6 and 10 years of experience using the Internet.

Procedures

Participants were recruited from an urban university and asked to complete an anonymous survey regarding their computer use, thoughts and feelings. Informed consent was obtained from students for use of anonymous data. Participation was voluntary, and all students were informed that participation (or refusal to participate) would not affect their course grade. Our Institutional Review Board (IRB) reviewed study procedures and approved the study. Measures were completed in a group classroom setting under the supervision of trained research assistants.

Measures

iSECURE

An original 20-item instrument asks participants to rate the frequency with which they engage in such behaviours along a four-point Likert-type scale ('Never', 'Rarely', 'Sometimes' and 'Often'). Items were developed by the authors and crafted to represent generally secure or unsecure cyber activities, for example, secure, 'I download virus protection updates'; insecure, 'I use unsecured wireless ("Wi-Fi") networks'. iSECURE psychometrics are a focus of the current study and are described below (see the 'Results' section). Items were developed via discussions with team members and others in the secure computing community. Items also drew from the measures developed by Halevi et al. [8] and McBride et al. [1] and are each designed to assess participants' secure and insecure online activity. An original item pool for the iSECURE drew from online security recommendations made by various university information technology departments, Internet service providers, security software firms and the United States-Computer Emergency Readiness Team. We limited ourselves to those recommendations intended for end users, rather than systems administrators. These were crafted into reflective statements about user behaviour (e.g. 'I have…') that could be rated in terms of personal applicability. Our research team of cyber security and behavioural science experts reviewed these items in consultation with professionals and pared the set to a final list of 20 items.

Safe computing scales

A measure used by Anderson and Agarwal [6] was included as a means to assess construct validity of the iSECURE. Subscales include: level of concern regarding security threats, security behaviour self-efficacy, perceived citizen efficacy, subjective norms of

cyber security (i.e. peer beliefs about own security), descriptive norms of cyber security (i.e. own beliefs about others' security), and intentions and attitudes towards securing one's personal computer. Extant work with these subscales has found reliability estimates in the moderate to good range.

Big Five Inventory

The Big Five personality traits of openness, conscientiousness, extraversion, agreeableness, and neuroticism were assessed using the Big Five Inventory [15,16]. Respondents are presented with 44 human characteristics (e.g. 'Is original, comes up with new ideas') and asked to rate their personal applicability along a five-point scale (1 = 'Disagree Strongly', 5 = 'Agree Strongly'). Subscale scores are created by averaging responses to items representative of each personality trait. In the current study, internal consistency for each subscale ranged from acceptable to good (.72–.84).

Existential anxiety questionnaire

The existential anxiety questionnaire (EAQ) [17,18] is a 13-item measure of existential anxiety based on the Tillich conceptualisation of existential concerns [19]. The EAQ demonstrated acceptable internal consistency in this sample (α = .76).

Peer conflict scale – 20-item version (PCS-20)

The PCS-20 [20] is a self-report measure of aggressive behaviour. Consistent with extant research [21], PCS items demonstrated good internal consistency in this sample (α > .85).

State-trait anxiety inventory – form Y (STAI-Y)

The STAI-Y [22] is a 20-item self-report measure of anxiety symptoms. Specifically, the STAI is believed to differentiate between anxiety symptoms specific to the individual (trait) and those resulting from context (state). By extracting circumstance-derived anxiety from global assessment, the STAI permits a more accurate assessment of relatively stable trait anxiety. Participants respond along a four-point intensity scale ranging from 'not at all' to 'very much so'. Research using the STAI-Y has continued to find that it demonstrates good reliability (αs >.85 [23]).

Brief symptom inventory (BSI-18)

Participants were screened for symptoms of psychological disorder and distress using the BSI 18 [24], an 18-item self-report measure. The BSI 18 includes subscales assessing broad symptom dimensions of somatisation, depression and anxiety. Internal consistency estimates of individual subscales indicate good reliability (αs >.70 [24]).

Inventory of callous–unemotional traits (ICU)

Callous and emotional traits were measured using the appropriately named ICU ([25]), a 24-item self-report inventory. Essau et al. [26] report good reliability for the ICU overall (α < .70), as well as the callousness and uncaring subscales, though only an acceptable level of reliability for the unemotional factor (α = .64).

Results

Distributions of the two iSECURE scales (presented in Figures 1 and 2) suggest that there is a negative skew in secure cyber behaviours (i.e. more in the high secure tail of the distribution), in that participants tended to believe they engaged in more secure cyber behaviour. In contrast, insecure behaviour is normally distributed, with a few individuals

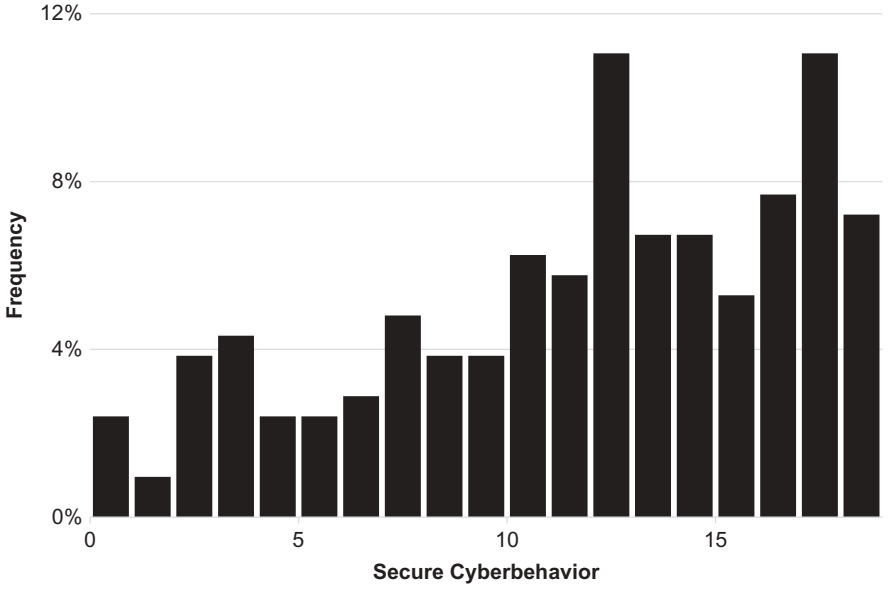

Figure 1. Frequency distribution of iSECURE secure cyber behaviour subscale scores.

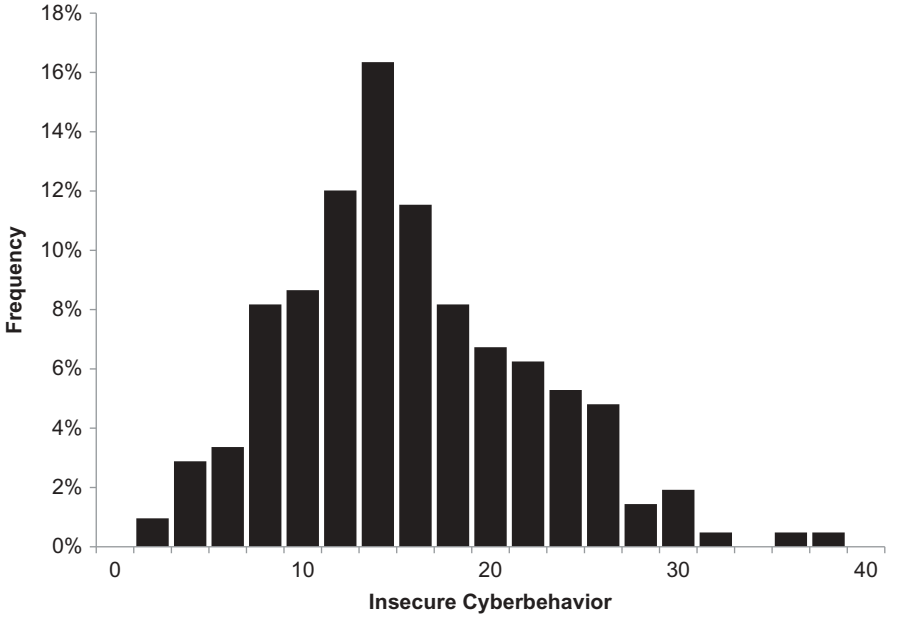

Figure 2. Frequency distribution of iSECURE insecure cyber behaviour subscale scores.

showing very high risk. Descriptive statistics for other variables of interest are presented in Table 1. The factor structure of the iSECURE was examined using exploratory factor analysis, with the intention of determining the most theoretically consistent structure, while minimising cross loadings. Missing data were handled using pairwise deletion of cases as suggested by Tabachnick and Fidell [27].

Factorability was appropriate because of both the sample size and the observed patterns of intercorrelation among items (i.e. numerous inter-item correlations exceeded .30). A non-significant sphericity test, $\chi^2(190) = 1620.40$, $p < .001$, and acceptable Kaiser–Meyer–Olkin sampling adequacy (.775), further signified that our data were comprised of common factors [27]. The number of factors was initially identified according to Kaiser's criterion (eigenvalues greater than one), then limited through visual inspection of a scree plot as recommended by Preacher and MacCallum [28]. We interpreted factor loadings with values above .32 as representative of salient indicators [27].

Exploratory factor analysis was conducted with principal axis factoring of the item correlation matrix using a Varimax rotation to simplify factor identification. An initial solution contained seven factors with eigenvalues greater than one. However, inspection of the scree plot revealed a steep descent from the second to third factors, suggesting the adequacy of a two-factor solution. Consistent with this, a two-factor solution accounted for 39% of variance in scores. Inspection of factor loadings found the solution to be theoretically sound, with items aligned with the posited factors of secure and unsecure cyber behaviour (see Table 2). Using the two-factor structure, mean levels of secure or unsecure behaviour were determined and are presented alongside other variables of interest in Table 1.

Construct validity for iSECURE factors was assessed by correlating mean scores of secure and unsecure cyber behaviour with the safe computing subscales

Table 1. Means, standard deviations and ranges for the variables of interest.

	Mean (SD)	Range
Secure behaviour	11.26 (5.03)	0–18
Insecure behaviour	15.12 (6.58)	0–38
Openness	36.08 (6.23)	0–50
Conscientiousness	30.58 (5.37)	0–45
Extraversion	26.06 (6.48)	0–40
Agreeableness	34.34 (5.85)	0–45
Neuroticism	23.51 (6.90)	0–40
Trait anxiety	43.66 (11.20	0–75
Fear\death concerns	1.92 (1.58)	0–5
Emptiness\meaninglessness concerns	1.60 (1.11)	0–4
Guilt\condemnation concerns	1.54 (1.21)	0–4
Somatisation symptoms	5.05 (5.26)	0–24
Anxiety symptoms	6.28 (6.34)	0–24
Depression symptoms	5.92 (6.11)	0–24
Aggression	5.99 (7.42)	0–80
Callousness	6.67 (4.05)	0–44
Uncaring	7.22 (4.99)	0–32
Unemotional	7.93 (3.61)	0–20
Cyber security concern	38.54 (12.41)	0–56
Security behaviour efficacy	23.12 (6.73)	0–35
Perceived citizen efficacy	16.72 (3.42)	0–28
Subjective norms of security	12.38 (4.78)	0–21
Attitude regarding security	17.07 (3.71)	0–21
Intentions regarding security	15.65 (4.31)	0–21

Table 2. Summary of results from an exploratory two-factor model of iSECURE items.

Item	Factor 1: Secure	Factor 2: Insecure	Mean (SD)	% endorsing
1. I use Facebook, Instagram, Google+, Twitter or another social media site	.111	.104	2.58 (0.78)	96.2
2. I download security updates for my computer	**.796**	.034	1.66 (1.03)	82.2
3. I download general software updates.	**.564**	.123	2.11 (0.94)	91.3
4. I use antivirus\anti-malware software on my computer	**.823**	−.031	2.11 (1.11)	85.0
5. I download virus protection updates	**.899**	.005	1.79 (1.13)	79.8
6. I use antivirus\malware software on my computer	**.854**	.020	2.05 (1.12)	84.5
7. I have accessed the private information of others using the computer/Internet	.232	**.361**	0.57 (0.91)	34.1
8. I have downloaded movies, music, videos, other media, etc. from 'share' sites	.016	**.440**	1.93 (1.05)	87.5
9. I use unsecure wireless 'Wi-Fi' networks	−.045	**.596**	1.47 (1.13)	74.9
10. I have accessed others' wireless 'Wi-Fi' networks without their consent	−.113	**.594**	1.22 (1.12)	64.9
11. I have accessed secure private wireless 'Wi-Fi' networks without their consent	.002	**.635**	0.58 (0.97)	32.2
12. I would use software to access private/secure sites if there was a good reason	.046	**.533**	1.01 (1.06)	57.7
13. I would use software to access private/secure sites	.122	**.600**	0.61 (0.90)	37.9
14. I have downloaded malicious software by accident	.247	**.380**	0.88 (0.87)	61.5
15. I have accessed Internet sites that my browser warned me may be insecure.	.069	**.457**	1.64 (0.95)	86.5
16. I download software and security updates as soon as they become available	**.537**	.091	1.53 (0.96)	83.2
17. I have illegally downloaded software or music online	−.007	**.572**	1.87 (1.13)	83.7
18. I have used\would use a work computer to look up information about friends\family	.170	**.344**	1.28 (1.06)	69.7
19. I regularly give out my email address	.017	.209	1.75 (0.94)	91.3
20. I have had a problem with malware on my computer in the past year	.183	**.350**	0.80 (0.95)	51.4

Bold values denote loadings > 0.32.

adapted by Anderson and Agarwal (Table 3). Notably, secure cyber behaviour showed significant positive associations with security behaviour self-efficacy (r = .39, p < .001), subjective norms about cyber security (r = .20, p < .01). Individuals engaging in secure cyber behaviours were more likely to report a positive attitude towards performing security-related behaviour (r = .24, p < .01), as well as greater intentions to perform such behaviour (r = .35, p < .001).

We continued by examining correlations between secure and insecure subscale scores and Big Five personality traits (Table 4) as well as aggression, anxiety, callous–unemotional traits and mental health symptoms (Table 5). Engagement in secure

Table 3. Associations between security-related cyber behaviours and safe computing subscales.

	1	2	3	4	5	6	8
1. Secure behaviour	–	–	–	–	–	–	–
2. Unsecure behaviour	.29**	–	–	–	–	–	–
3. Concern about security	.12	.08	–	–	–	–	–
4. Security behaviour self-efficacy	.39**	.13	.16*	–	–	–	–
5. Perceived citizen efficacy	.07	.14*	.25**	.15*	–	–	–
6. Subjective norm	.20**	.05	.43**	.25**	.22**	–	–
7. Attitude towards security	.24**	.02	.29**	.27**	.14	.33**	–
8. Intentions regarding security	.35**	.03	.24**	.42**	.15*	.39**	.62**

*p < .05.
**p < .01.

Table 4. Associations between security-related cyber behaviours and Big Five personality traits.

	1	2	3	4	5	6
1. Secure cyber behaviour	–	–	–	–	–	–
2. Insecure cyber behaviour	.29**	–	–	–	–	–
3. Openness	.05	.02	–	–	–	–
4. Conscientiousness	.09	−.23**	.25**	–	–	–
5. Extraversion	.01	.12	.25**	.15*	–	–
6. Agreeableness	.08	−.11	.09	.36**	.14*	–
7. Neuroticism	−.14*	.05	−.14*	−.22**	−.41**	−.19**

*$p < .05$.
**$p < .01$.

Table 5. Associations between security-related cyber behaviours, aggression, trait anxiety, mental health symptoms, callous–unemotional traits and existential anxiety.

	1	2	3	4	5	6	7	8	9	10	11	12
1. Secure cyber behaviour	–	–	–	–	–	–	–	–	–	–	–	–
2. Insecure cyber behaviour	.29**	–	–	–	–	–	–	–	–	–	–	–
3. Aggressive behaviour	−.11	.16*	–	–	–	–	–	–	–	–	–	–
4. Trait anxiety	−.13	.18*	.24**	–	–	–	–	–	–	–	–	–
5. Somatic symptoms	−.12	.17*	.30**	.57**	–	–	–	–	–	–	–	–
6. Anxiety symptoms	−.14	.13	.30**	.76**	.67**	–	–	–	–	–	–	–
7. Depressive symptoms	−.14	.18*	.29**	.75**	.77**	.85**	–	–	–	–	–	–
8. Callous	−.02	.08	.51**	.08	.15	.21**	.16*	–	–	–	–	–
9. Uncaring	.05	.15*	.22**	.10	−.05	.02	−.06	.26**	–	–	–	–
10. Unemotional	.06	.03	.06	.10	−.08	.10	.02	.11	.25**	–	–	–
11. Fear\death	−.04	.06	.20**	.50**	.32**	.47**	.47**	.11	.07	.03	–	–
12. Emptiness \meaninglessness	−.14	.15*	.26**	.54**	.40**	.54**	.49**	.17*	.16*	.04	.47**	–
13. Guilt\condemnation	−.07	.12*	.14	.44**	.43**	.46**	.51**	.13	−.00	.02	.35**	.39**

*$p < .05$.
**$p < .01$.

cyber behaviours was associated with lower levels of neuroticism ($r = -.14$, $p < .05$), and fewer mental health symptoms ($r = -.14$), though this effect was only marginally significant ($p = .051$). However, secure cyber behaviour practices were linked to greater concerns about emptiness and meaninglessness in one's life. Conversely, insecure cyber behaviours were associated with lower levels of conscientiousness ($r = -.23$, $p < .01$; Figure 3), increased report of somatic ($r = .19$, $p < .01$) and depressive symptoms ($r = .22$, $p < .01$), as well as higher levels of aggressive behaviour ($r = .16$, $p < .05$). Insecure cyber behaviour was linked to a generally uncaring nature ($r = .15$, $p < .05$), though also associated with existential concerns about guilt and condemnation ($r = .19$, $p < .05$).

Discussion

The current paper provided initial data on a new measure, the iSECURE, for assessing security in cyber behaviour. First, the distributions of the two iSECURE scales (presented in Figures 1 and 2) suggest that there is a skew towards people thinking they are secure (i.e. more in the high secure tail of the distribution), but that insecure behaviour is normally distributed with possibly a few of very high risk. A general tendency in the population towards feeling more secure is an interesting finding deserving more scrutiny. That is, people may actually be secure or they may have a bias towards feeling more secure than

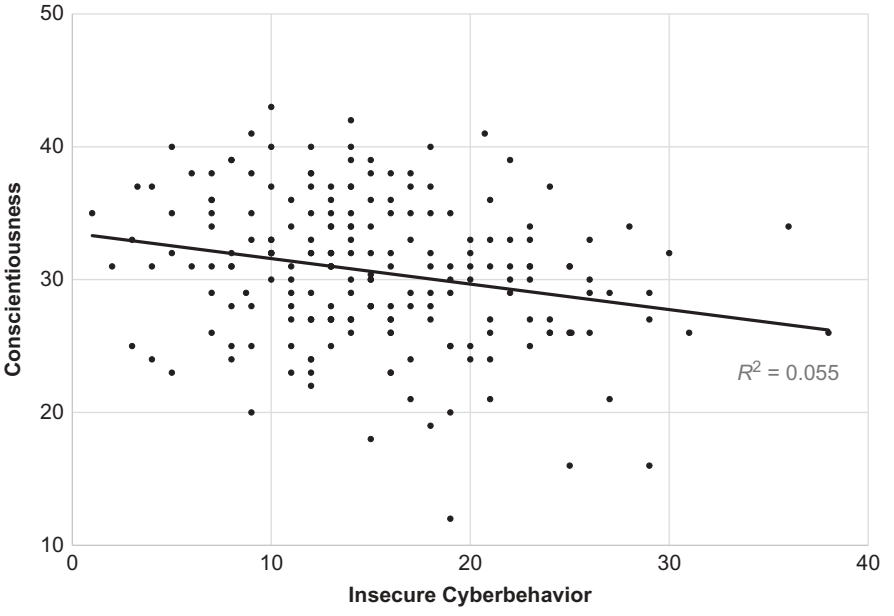

Figure 3. Negative association between conscientiousness and insecure cyber behaviour.

they really are. Interestingly, mean scores on the insecure behaviour subscale generally followed a normal distribution. This suggests that individuals may indeed be willing to admit engaging in insecure or even unethical cyber behaviours. Here, we believe that our use of anonymous data collection methods may have contributed to reducing social desirability bias among our respondents. Many researchers have demonstrated the efficacy of self-report measures in assessing socially undesirable behaviours (e.g. [20,25]), often using anonymous collection methods. However, until now, the appropriateness of self-report methods to deviant cyber behaviour remained untested.

Correlating the secure and insecure factors against extant measures of behavioural cyber security, we found support for the construct validity of the iSECURE subscales. Specifically, secure cyber behaviours were positively associated with beliefs about personal efficacy in protecting oneself online, as well as shared subjective norms about cyber security, and a positive attitude about cyber secure behaviour. In contrast, and consistent with theory, these associations were not observed for insecure behaviour. These findings support the construct validity of the iSECURE. Specifically, we demonstrate that beliefs and attitudes about cyber security are linked to the hypothesised iSECURE factors in a manner consistent with theory.

Drawing from extant research, and noting conflicting results in previous studies, we chose to examine associations between iSECURE subscales and Big Five personality traits. Interestingly, and contrary to our hypothesis, neuroticism was negatively correlated with secure cyber behaviours. We anticipated that individuals high in neuroticism would be more attuned to cyber risk and thus more likely to engage in secure behaviour. Logically, this follows from neuroticism's general association with worrisome, anxious thoughts, and evidence suggesting that neurotic individuals tend to be more cognizant of threatening cues [29]. However, our results suggest the opposite. That is, neurotic individuals are *less*

likely to practise secure cyber behaviours, though no more likely to engage in insecure behaviours. Potentially, the anxiety and worry common among individuals high in neuroticism may limit the mental resources that can be devoted to maintaining cyber security. Relatedly, individuals high in conscientiousness were less likely to engage in insecure cyber behaviours. Such an association makes theoretical sense, given that conscientious individuals are characterised by a tendency to obey rules, act responsibly and behave in an ethical manner [30]. A conscientious person would therefore be less likely to engage in potentially harmful or unjust cyber behaviour.

We further identified that aggression, depression and trait anxiety are positively and significantly correlated (each accounting for about 3–5% of variance) with the insecure behaviour scale, suggesting that those with anxiety, depression and high aggression are more likely to engage in insecure cyber behaviours. We have also found that the secure behaviour scale is significantly negatively correlated with neuroticism and existential concerns about the meaning of life, suggesting that the more you have a positive sense of your place in the world and are generally happy the more likely you are to engage in secure cyber behaviour. Further testing of these associations is needed.

Several limitations of the current study should be acknowledged. First, the cross-sectional nature of our investigation precludes any analysis of potential change in cyber security behaviours over time. Therefore, research is needed to examine the stability of such behaviours, as well as the test–retest reliability of the iSECURE. Second, our use of a college-age sample may limit generalisability to the broader work force population. Continuing study of the iSECURE might involve the testing of measurement invariance across age, or other demographic characteristics. Third, this study relies solely on results gathered from self-report instruments. Therefore, our results suffer from shared method variance. Research is needed that examines the iSECURE in relation to real-world behaviours.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the National Science Foundation under award number 1358723.

Notes on contributors

Justin D. Russell, MS, is a doctoral candidate in the Department of Psychology at Iowa State University. He received his B.A. from the University of Rochester, and his M.S. from the University of New Orleans. He is interested in exploring the utility of psychological science to understand and mitigate the human role in cyber security vulnerability.

Carl F. Weems, Ph.D., is a professor and chair of the Department of Human Development and Family Studies at Iowa State University. He received his Ph.D. from Florida International University. His interests focus on emotional development as well as the intersection of personality traits, mental health and human behaviours in relation to cyber security.

Irfan Ahmed, Ph.D., is an assistant professor in the Department of Computer Science at the University of New Orleans. He received his Ph.D. in computer science from Ajou University in Suwon, South Korea. His work has focused on issues related to human factors in cyber security, digital forensics and cyber security education.

Golden G. Richard III, Ph.D., is a professor in the Division of Computer Science and Engineering at Louisiana State University. He completed his Ph.D. in computer science from The Ohio State University. His research interests focus on topics related to digital forensics, memory forensics, reverse engineering, malware analysis and operating systems.

References

1. McBride M, Carter L, Warkentin M Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. RTI International-Institute for Homeland Security Solutions; 2012.
2. Thomas GF, Kuper SR, Thomas KM, et al. Understanding the user can be a tool for cyber defense. DTIC Document; 2012.
3. West R. The psychology of security. Commun ACM. 2008;51:34–40.
4. Kopstein J 'Cybersecurity': how do you protect something you can't define? [Internet]. The Verge. 2012. [cited 2015 Aug 17]. Available from: http://www.theverge.com/policy/2012/8/22/3258061/defining-cybersecurity-fud-cispa-privacy
5. Committee on National Security Systems Glossary Working Group. National Information Assurance Glossary [Internet]. 2010. Available from: http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf
6. Anderson CL, Agarwal R. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. Mis Q. 2010;34:613–643.
7. Crossler RE, Johnston AC, Lowry PB, et al. Future directions for behavioral information security research. Comput Secur. 2013;32:90–101.
8. Halevi T, Lewis J, Memon N A pilot study of cyber security and privacy related behavior and personality traits. Proceedings of the 22nd International World Wide Web Conference. Rio de Janeiro, Brazil: International World Wide Web Conferences Steering Committee; 2013. p. 737–744.
9. Korzaan ML, Boswell KT. The influence of personality traits and information privacy concerns on behavioral intentions. J Comput Inf Syst. 2008;48:15–24.
10. Warkentin M, McBride M, Carter L, et al. The role of individual characteristics on insider abuse intentions. AMCIS 2012 Proc. [Internet]. Association for Information Systems; 2012. Available from: http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/28
11. Bègue L, Beauvois J-L, Courbet D, et al. Personality predicts obedience in a Milgram paradigm. J Pers. 2015;83:299–306.
12. Mashiko H. The relationship between the tendency of over-adaptation and personality traits, fears of abandonment, and approval motivation in adolescence. Jpn J Couns Sci. 2008;41:151–160.
13. Frick PJ. Developmental pathways to conduct disorder: implications for future directions in research, assessment, and treatment. J Clin Child Adolesc Psychol. 2012;41:378–389.
14. Kimonis ER, Branch J, Hagman B, et al. The psychometric properties of the Inventory of Callous–Unemotional Traits in an undergraduate sample. Psychol Assess. 2013;25:84–93.
15. John OP, Donahue EM, Kentle RL. The Big Five Inventory - Versions 4a and 54. Berkeley, CA: University of California, Berkeley, Institute of Personality and Social Research; 1991.
16. John OP, Naumann LP, Soto CJ. Paradigm shift to the integrative Big Five trait taxonomy: history, measurement, and conceptual issues. In: John OP, Robins RW, Pervin LA, editors. Handbook of personality theory and research. New York, NY: Guilford Press; 2008. p. 114–158.
17. Scott BG, Weems CF. Natural disasters and existential concerns: a test of Tillich's theory of existential anxiety. J Humanist Psychol. 2013;53:114–128.

18. Weems CF, Costa NM, Dehon C, et al. Paul Tillich's theory of existential anxiety: a preliminary conceptual and empirical examination. Anxiety Stress Coping. 2004;17:383–399.
19. Tillich P. The courage to be. New Haven, CT: Yale University Press; 1952.
20. Marsee MA, Barry CT, Childs KK, et al. Assessing the forms and functions of aggression using self-report: factor structure and invariance of the Peer Conflict Scale in youths. Psychol Assess. 2011;23:792–804.
21. Scott BG, Lapré GE, Marsee MA, et al. Aggressive behavior and its associations with posttraumatic stress and academic achievement following a natural disaster. J Clin Child Adolesc Psychol. 2014;43:43–50.
22. Spielberger CD, Gorsuch RL, Lushene PR, et al. Manual for the state-trait anxiety inventory. Palo Alto, CA: Consulting Psychologists Press; 1983.
23. Barnes LL, Harp D, Jung WS. Reliability generalization of scores on the Spielberger state-trait anxiety inventory. Educ Psychol Meas. 2002;62:603–618.
24. Derogatis LR. The Brief Symptom Inventory-18 (BSI-18): administration, scoring, and procedures manual. 3rd ed. Minneapolis, MN: National Computer Systems; 2000.
25. Kimonis ER, Frick PJ, Munoz LC, et al. Callous-unemotional traits and the emotional processing of distress cues in detained boys: testing the moderating role of aggression, exposure to community violence, and histories of abuse. Dev Psychopathol. 2008;20:569–589.
26. Essau CA, Sasagawa S, Frick PJ. Callous-unemotional traits in a community sample of adolescents. Assessment. 2006;13:454–469.
27. Tabachnick BG, Fidell LS. Using multivariate statistics. 5th ed. Boston, MA: Pearson Education Inc.; 2007.
28. Preacher KJ, MacCallum RC. Repairing Tom Swift's electric factor analysis machine. Underst Stat Stat Issues Psychol Educ Soc Sci. 2003;2:13–43.
29. Gray JA. Brain systems that mediate both emotion and cognition. Cogn Emot. 1990;4:269–288.
30. Costa PT, McCrae RR, Dye DA. Facet scales for agreeableness and conscientiousness: a revision of the NEO personality inventory. Personal Individ Differ. 1991;12:887–898.