Transactions on Replication Research

Methodological Replication DOI: 10.17705/1atrr.00074 ISSN 2473-3458

A Replication Study of the Impact of Impulsivity on Risky Cybersecurity Behaviors

Zahra Aivazpour
Department of MHRIS
California Polytechnic State University
San Luis Obispo
zaivazpo@calpoly.edu

V. Srinivasan (Chino) Rao
Department of Information Systems & Cybersecurity
University of Texas at San Antonio
Chino.rao@utsa.edu

Abstract:

Hadlington (2017) conducted a survey using respondents from the United Kingdom (UK) to examine the relationship between the three dimensions of impulsivity and risky cybersecurity behavior. His results showed that risky cybersecurity behavior was positively correlated to attentional impulsivity and motor impulsivity, but was negatively correlated with non-planning impulsivity. He also examined the relationship between internet addiction and attitude towards cybersecurity and risky cybersecurity behaviors. Our longer term goal is to conduct research to gain an in-depth understanding of the role of impulsivity in cybersecurity. Towards this end, we conducted a methodological replication of the Hadlington study to determine the generalizability of his results for respondents from a different country, i.e., the USA. Our replication confirmed most of the correlations between the variables in Hadlington's study, though there are some differences that need further examination. We further explored the data in search of meaningful patterns in risky cybersecurity behaviors scale and its relationship with different impulsivity components. Our exploratory analysis suggests a need for a typology of cybersecurity behaviors. Overall, we see a sufficient basis to pursue research on the effects of impulsivity on risky security behaviors.

Keywords: Impulsivity, Risky Cybersecurity Behaviors, Replication.

The manuscript was received 12/10/2020 and was with the authors 8 months for 2 revisions.

1 Introduction

The influence of personality characteristics on cybersecurity behaviors is a topic of interest to information systems researchers (e.g., Shropshire, Warkentin, Johnston & Schmidt, 2006). For example, the influence of Big Five personality factors on cybersecurity behaviors has been studied by Kennison and Chan-Tin (2020) and that of psychopathy by Maasberg, Warren, and Beebe (2015). The role of impulsivity in understanding security behavior has also been studied (e.g., Egelman & Peer, 2015a), but has otherwise received limited attention. Impulsivity is 'the urge to act spontaneously without reflecting on an action and its consequences' (Coutlee, Politzer, Hoyle, & Huettel, 2014, p. 2). Its relevance to cybersecurity can be readily argued. For instance, a more impulsive person may be likelier to click on a phishing link (e.g., Butavicius, Parsons, Pattinson, & McCormac, 2016), or share a password with a friend or acquaintance, both of which are considered risky cybersecurity behaviors. Thus, a study of the role of impulsivity on cybersecurity behaviors is important.

Hadlington (2017) conducted a survey to enhance the understanding of the relationship between impulsivity and risky cybersecurity behaviors. Impulsivity was viewed as a three-dimensional construct based on the work of Patton, Stanford and Barratt (1995). The three dimensions are as follows: attentional impulsivity, which refers to cognitive instability and the inability to focus on the tasks at hand; motor impulsivity, which refers to the tendency to engage in actions on the spur of the moment; and, non-planning, which impulsivity refers to the inability to plan complex mental tasks. Risky cybersecurity behavior (RScB) refers to engagement in behaviors that are generally known to increase the vulnerability of personal or organizational information assets. It also includes non-engagement in behaviors generally known to decrease the vulnerability of personal or organizational information assets. In effect, risky behaviors correspond to engagement in those acts that are listed as unsafe and prohibited, or, non-engagement in those acts that are listed as beneficial and recommended in compliance guidelines of organizations. In addition to examining the effect of impulsivity, Hadlington also examined the relationship between two other variables and RScB. These two variables were internet addiction (using an online cognition scale (OCS)) and attitude towards cybersecurity (using the attitude towards cybersecurity and cybercrime in business scale (ATC-IB)).

The purpose of the current study is to conduct a methodological replication (following the classifications provided in Dennis and Valacich (2014)) of the Hadlington (2017) study to generalize his results, using a respondent sample from a different country. The Hadlington study was done using respondents from the United Kingdom (UK). The majority of our respondents are from the United States of America (USA). While our primary interest is on the role of impulsivity, we replicated Hadlington's study completely, and report the results herein.

In addition to the replication, we conduct two explorations of the data. One, we conduct an exploratory factor analysis (EFA) of the risky cybersecurity behavior items in search of clusters around which to develop typologies. Two, we explore the correlation coefficients of each individual risky cybersecurity behavior to the three dimensions of impulsivity in an effort to understand how different behaviors are affected by impulsivity.

We divide our article into six sections. In section 2, we provide our reasoning for replication and discuss the replication type and in section 3 we provide a summary of the original results and compare them to our replication results. We discuss the key findings of the two studies and explore possible explanations for observed differences in section 4. In section 5, we report the results of the EFA and discuss the correlation results. In the last section, we provide concluding remarks.

2 Background for Replication & Replication Type

The relevant background for our replication includes three issues: (a) the need to use a targeted variable for prediction in preference to the more general Big Five personality factors, (b) the choice of the impulsivity scale, and, (c) the choice of the study for replication. We discuss each of these issues below. Further, we present a more nuanced discussion of the classification of the replication type.

The relationship between personality characteristics and security behaviors is an area of research interest in information systems. General personality scales, such as The "Big Five" traits (Borgatta, 1964) are often used as the predictor personality characteristics (Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018). It has been argued that targeted traits may be stronger predictors of specific behaviors than the general personality scales (Egelman & Peer, 2015a). Egelman and Peer have shown that decision making style

and risk taking attitudes are better predictors of privacy attitudes than the five factor model. Based on this, we believe that impulsivity will be a better predictor of some security behaviors and plan to examine the domain in greater detail in our broader program of research. As a starting point, we replicated a study involving impulsivity and security behaviors.

A direct scale is often used to measure impulsivity in studies of security behaviors that hypothesize an explanatory role for impulsivity (e.g., Barratt Impulsivity Scale (BIS) (see Patton et al., (1995) for discussion of scale)). The Barratt Impulsivity Scale (BIS) is a freestanding measure (i.e., not a subset of another measure), which is directly focused on measuring impulsivity. The scale has been used in two studies (Egelman & Peer, 2015a; Hadlington, 2017). The studies have shown that impulsivity influences security related intentions/behaviors. The BIS scale (Patton et al., 1995) and abbreviated BIS scales (Coutlee et al., 2014) are well established scales, and their limited use-to-date in security-related studies have shown promising results. The choice of the scale is therefore appropriate. Additional studies, such as our replication, would serve to establish the robustness of the scale.

Our choice of studies to replicate was limited to the two available studies (Egelman & Peer, 2015a; Hadlington, 2017) using the impulsivity scale, which indicated a correlation between impulsivity and security-related intentions/behaviors. Egelman and Peer studied the effect of impulsivity on security behavior intentions. Hadlington studied the effect of impulsivity on security behaviors, as measured by participant recall. We chose to replicate the Hadlington study on behaviors rather than the Egelman and Peer study on intentions.

Earlier, we have stated that our study is a methodological replication, based on a strict application of the categorization of replications proposed by Dennis and Valacich (2014). We use identical measures, treatments, statistics, etc. as the Hadlington (2017) study, and conduct the replication in the US context versus the UK context of the original study. It should be pointed out that despite the different national contexts of the two studies, there are similarities in the social and business norms of the two contexts. We mention this for the sake of completeness.

Overall, our primary purpose for the replication is to generalize the results from the UK context to the US context. We have additionally explained how the Hadlington (2017) study was appropriate for our replication, given our interest in the relationship between a targeted trait (i.e., impulsivity) and security-related behaviors.

3 Summary of Original Study & Replication Results

The original study by Hadlington (2017) was conducted in the United Kingdom (UK). Participants completed an online survey. Participants were full-time or part-time employees. Five hundred and fifteen usable responses were collected. The survey included scales for four variables: abbreviated impulsiveness scale (ABIS) and online cognition scale (OCS) to measure internet addiction, risky cybersecurity behaviors (RScB), and attitude towards cybersecurity and cybercrime in business (ATC-IB). The items used in the replication study for all the scales are shown in Appendix A.

For ABIS, a modified version of the 13-item impulsivity scale proposed by Coutlee et al. (2014) was used. The ABIS is based on the original 30-item Barratt's Impulsiveness Scale (see Patton et al., 1995). Scoring of items was done using a 4-point scale (1=never/rarely to 4=almost always/always). Internet addiction was measured using the OCS developed by Davis, Flett, and Besser (2002). It was scored using a 7-point Likert scale (1= strongly agree to 7=strongly disagree). This scale comprises four dimensions: social comfort, loneliness, diminished impulse, and distraction. In the analyses, the scale is treated as a unidimensional measure. Risky cybersecurity behavior is measured using a 20-item scale. This is partially based on the security behaviors intentions scale (SeBIS) developed by Egelman and Peer (2015a, 2015b). The RScB scale asked participants to state how often they had engaged in a particular unsafe cybersecurity activity during a previous six-month period. It was scored on a 7-point scale (0=never to 6=daily). To measure attitude, Hadlington developed the ATC-IB scale, in which high scores on the measurement indicate positive attitude toward cybersecurity behavior. "The scale was constructed to reflect a wide spectrum of attitudes towards both cybersecurity and cybercrime within a business context" (Hadlington, 2017, p. 7). This scale was scored on a 4-point Likert scale (1=strongly disagree to 4=strongly agree). Hadlington (2017) states that each of the scales had high internal validity scores.

The replication study was conducted in the United States using MTurk as a vehicle to recruit participants. Participants completed an online survey. Participant demographics are shown in Table 1.

Table 1. Demographics of Respondents		
Demographic	**Category**	**Percent**
Gender	Male	44.8
	Female	55.2
Age	20-25	16.3
	26-30	30.0
	31-35	13.3
	36-40	13.3
	40+	26.3
Ethnicity	Caucasian	61.1
	Asian	27.5
	African American	4.9
	Other	6.6
Education	Less than high school	0.8
	High School	19.7
	College	51.5
	Graduate	28.0

Respondents could withdraw from the survey at any time without any penalty. Trap questions were embedded in the questionnaire to remove surveys in which participants appeared to have responded randomly. A total of two hundred and fifty-one participants completed the survey. Two hundred and forty-five usable responses were collected. The six surveys that were dropped failed to answer the trap questions correctly. The response rate is not relevant as recruitment was through an open call and not through solicitation of a specific number of individuals. We used the original 13-item ABIS impulsivity scale (see Coutlee et al., 2014) to measure three dimensions of impulsivity, in contrast to the modified scale used in the original study. We did not realize that the scale had been modified in Hadlington (2017) prior to data gathering. Only two items are different between the scale that we used and the one used in the original research. All other scales are the same as the original study. Cronbach's alpha for all the measurement scales and sub-scales was higher than 0.7 cut-off point; therefore, no item was dropped from the survey questionnaire.

The results of average correlations for both the original and replicated studies are shown in Table 2. The results of the replicated study are shown using bold text. Both studies show that both attentional impulsivity and motor impulsivity are correlated to risky cybersecurity behavior, correlations which are as expected, but the correlation coefficients are higher in the replicated study. Non-planning impulsivity is negatively correlated to RScB in the original study, which is contrary to expectations and difficult to explain. In the replicated study, non-planning impulsivity is not correlated to RScB. In both studies, all three dimensions of impulsivity are negatively correlated to attitude to cybersecurity (ATC-IB) (i.e., high impulsivity corresponds to negative attitude, and this is consistent with expectations).

Table 2. Comparison of Correlation Coefficients between Original and Replicated Studies					
	Impulsivity Attention	Impulsivity Motor	Impulsivity Non-Planning	ATC-IB	OCS
Impulsivity Attention					
Impulsivity Motor	0.36** **0.43****				
Impulsivity Non-Planning	0.60** **0.58****	0.14** **0.35****			
ATC-IB	-0.24** **-0.27****	-0.24** **-0.53****	-0.11* **-0.21****		
OCS	0.21** **0.26****	0.35** **0.48****	0.00 **0.15***	-0.40** **-0.54****	
RScB	0.15** **0.23****	0.30** **0.65****	-0.30[a] **0.07**	-0.30** **-0.70****	0.36** **0.61****
**p<0.01; * p<0.05; a= p-value not indicated in original.					

The original study also reported two other analyses: a hierarchical regression to assess internet addiction (using the online cognition scale, OCS) and attitude to cybersecurity (ATC-IB) as predictors of RScB (see Table 3), and a linear model for the effect of impulsivity subscales as predictors of risky cybersecurity behaviors (see Table 4). The hierarchical regression to examine the explanatory powers of internet addiction and attitude to cybersecurity as predictors of risky cybersecurity behaviors for both studies are shown in Table 3 (results of replication shown in bold). Both internet addiction and attitude to cybersecurity and cybercrime significantly predict risky cybersecurity behavior. No major difference is seen between the results of the replicated and original study.

Table 3. Comparison of Original and Replicated Models of OCS and ATC-IB as predictors of RScB

	B	**p-value**
Step 1		
Constant	6.57 **-0.72**	0.001
OCS	0.14 **0.64**	0.000
Step 2		
Constant	32.89 **4.81**	0.000
OCS	0.14 **0.34**	0.000
ATC-IB	-0.38 **-1.63**	0.000

The results of regression analysis for three dimensions of impulsivity for both studies are shown in Table 4 (results of replication study shown in bold). Both motor and non-planning impulsivities were significant predictors of RScB in both studies, but attentional impulsivity was a significant predictor in the original study but not in the replication. This was curious because attentional impulsivity is positively correlated to risky cybersecurity behavior in the replication (see Table 2), Such discrepancies usually occur either due to multicollinearity or "suppression effect." In the replication, maximum variance inflation factor (VIF values) was less than 1.7 for the independent variables, indicating the absence of multicollinearity.

In Table 2, non-planning impulsivity has a weak correlation with risky cybersecurity behavior (correlation = 0.07, n.s.), but has a high correlation with attentional impulsivity (correlation coefficient = 0.59, $p<0.01$), suggesting that non-planning impulsivity may be suppressing the effects of attentional impulsivity.

Table 4. Linear Model for ABIS Subscales as predictors of RScB

	B	**p-value**
Constant	9.31 **0.25**	0.004 **0.236**
Attentional Impulsivity	3.73 **0.11**	0.02 **0.382**
Motor Impulsivity	6.64 **1.87**	.000 .000
Non- Planning Impulsivity	-2.90 **-0.38**	0.023 **0.001**
R square for original study: 0.096; R square for replicated study: **0.446**		

To test for suppression effect we use a hierarchical regression, adding the three subscales of impulsivity one by one. In the first model, with only non-planning impulsivity as the independent variable, the coefficient of non-planning is positive and non-significant (see Table 5). However, when attentional impulsivity is added (see Table 6), the coefficient for non-planning impulsivity changes sign (becomes negative) and is not significant. It should be noted that the variance explained by attentional impulsivity and non-planning impulsivity totals about 5% only. The total variance explained by all three impulsivity dimensions is close to 45% (see Table 4), indicating that motor impulsivity accounts for almost 40% of the

variance in risky cybersecurity behavior. A point of note is that the impulsivity dimensions explained only about 10% of the variance in RScB in the original study.

Table 5. Linear Model of Non-Planning Impulsivity as a Predictor of RScB

	B	P-value
Constant	1.52	.000
Non- Planning Impulsivity	0.13	0.283
The model is not significant; R square: 0.005		

Table 6. Linear Model of Non-Planning Impulsivity and Attentional Impulsivity as a Predictor of RScB

	B	P-value
Constant	1.06	.000
Non- Planning Impulsivity	-1.70	0.207
Attentional Impulsivity	0.60	.000
R square: 0.05		

In the next section, we compare the results of the replication with those of the original study.

4 Discussion of Replication

In the current study, we replicated Hadlington's examination of the relationship between risky cybersecurity behavior and three other variables: impulsivity, attitude to cybersecurity, and, internet addiction (online cognition scale) (Hadlington, 2017). Table 7 provides a summary comparison of the two studies, following the template used by D'Arcy, Bandi, Cukier, Dykstra, and Ginther (2018).

The comparison shows that both motor impulsivity and attentional impulsivity are significantly correlated to risky security behaviors in both studies. Non-planning impulsivity was not correlated to RScB in the replication but was in the original study. Of peripheral interest is that non-planning impulsivity was correlated to OCS in the replication but not in the original study. A significant point of difference between the two studies is 44.6% of the variance in RScB was explained in the impulsivity model in the replication, while only 9.6% of variance was explained in the original study. It can also be noted that motor impulsivity accounts for the bulk of the variance (about 40% of the 45% explained by the total model) in the replication.

Table 7. Summary of the Comparison between Original Study and Replication Study

Characteristics	Replication	Original Study
Data Collection	Cross-sectional survey	Cross-sectional survey
Survey Design	Online Questionnaire	Online Questionnaire
Population	MTurk workers	Part-time or full-time employment in the UK
Sampling	Participants recruited via MTurk	Participants recruited via an online questionnaire using Qualtrics Research Panel
Sample size	251 participants Usable responses:245	538 participants. Usable responses: 515
Demographics	Age: 20-60+; Male: 44.8%; Female: 55.2% (Table 1)	Age: 18 – 84; Males: 42.3%; Females: 57.7%
Analysis	Correlation; hierarchical regression	Correlation; hierarchical regression

Findings	Motor impulsivity correlated to RScB Attentional impulsivity correlated to RScB Non-planning impulsivity not correlated to RScB Non planning significantly correlated with OCS	Motor impulsivity correlated to RScB Attentional impulsivity correlated to RScB Non-planning impulsivity correlated to RScB Non planning is not correlated with OCS
R square for Impulsivity Model	44.6%	9.6%

In terms of understanding the effects of impulsivity on risky security behaviors, the key findings that emerge from both studies are: (a) impulsivity does correlate with risky security behaviors, and (b) motor impulsivity is the most important explanatory behavior. The correlation between impulsivity and risky security behaviors is consistent with correlations between impulsivity and other types of risky behaviors (e.g., gambling, (Langewisch & Frisch, 1998), drug use (Ryb, Dischinger, Kufera, & Read, 2006), and risky sexual behaviors (Winters, Botzet, Fahnhorst, Baumel, & Lee, 2009)). Motor impulsivity has been shown to have a marginally higher correlation than attentional or non-planning impulsivity to other behaviors (e.g, severity of alcohol dependence (Jakubczyk et al., 2013)). In general, motor impulsivity appears to reduce control in goal-directed behaviors (Hogarth, Chase & Baess, 2012). Our objective in conducting the replication was to examine the existence of a relationship between impulsivity and risky security-related behaviors. The results broadly confirm the existence of a correlation between impulsivity and risky security-related behaviors, but there are some differences between the two studies that need to be examined further.

The differences in results of the two studies are threefold. First, the replication study explained almost 45% of the variance in the risky security behavior in contrast to about 10% in the original study. Second, the correlations between most pairs of variables are higher in the replication than in the original study (see Table 2). Lastly, the effects of non-planning impulsivity are different in several cases between the two studies. Non-planning impulsivity was negatively correlated to risky cybersecurity behavior in the original, but no significant correlation was observed in the replication. There was no significant correlation between non-planning impulsivity and internet addiction (OCS) in the original, but a correlation was observed in the replication. In the regression analysis, non-planning impulsivity was suppressing the effect of attentional impulsivity in the replication, which was not observed in the original.

Of the three sets of differences, the most significant one is the difference in the extent of variance in risky security behavior explained in the two studies. The second difference relates to the correlations between variables. While the correlations in the replication are higher, the order of magnitude is not sufficiently different to cause concern. The third set of differences relates to non-planning impulsivity. The role of non-planning impulsivity in both studies is minimal, and hence the differences in correlations related to that variable are not of much importance. We limit our discussion to explanations of the differences in the total variance explained by impulsivity dimensions across the two studies.

We explore three possible explanations for the differences in the amount of variance explained in the two studies: sample size, cultural differences, and common method variance. Under common method variance, we address the possible effects of single source responses, and, social desirability bias. There is evidence that demographics, such as gender and age, have been shown to influence impulsivity scores (Chamberlain, Lust, & Grant, 2020). However, there is no clear difference in the demographics of the two samples, so that is not discussed as a possible source of differences in results between the two studies.

In terms of sample size, the original study had 515 usable responses; the replication had only 245 usable responses (out of 251). A smaller sample size might yield lower levels of significance of correlations. Statistical power is positively correlated with the sample size, which means that a larger sample size gives greater power (Suresh & Chandrashekara, 2012). However, in the current case, the significance levels in the replication study are comparable to, or higher than, the significance levels in the original study, despite the smaller sample size. Thus, the difference in sample size is unhelpful in explaining the differences in the results.

In terms of the location of the study, the original study was conducted in the UK, and the replication in the USA. An examination of the scores for Hofstede's cultural dimensions (Hofstede, 1980) shows only one key difference between the two countries. The score for long-term orientation for the UK is higher than the

score for the US. (51 vs. 26 [source: https://www.hofstede-insights.com/product/compare-countries/]). Long-term orientation has been shown to correlate positively with increased voluntary security actions (Aurigemma & Mattson, 2019). It may be argued that long-term orientation is more likely to lead to compliance with security policies (i.e., users are more willing to accept the short-term inconveniences of complying with the security policies for the longer term benefit of securing data). Thus, the RScB scores for UK subjects may vary less than the RScB scores for the US subjects. This would reduce the level of correlation between impulsivity scores and RScB for the original UK data in comparison to the replicated data from the US subjects. In other words, the cultural dimension of long-term orientation may be influencing the self-report responses of subjects to a different extent in the two groups. The inclusion of scales to measure the dimensions of the culture construct in future research, similar to the work done by Keil et al. (2000), would enable researchers to determine if cultural effects explain the differences in results between the original study and the replication.

Another explanation might be provided by the notion of common method variance (CMV). CMV is "variance that is attributable to the measurement method rather than to the constructs the measures represent" (Podsakoff et al., 2003, p. 879). The higher correlation in the replication sample could result from greater common method bias in the US sample, related to the use of a single source for the measurement of all variables. Admittedly, this is a possibility. However, there is no definitive argument to suggest that CMV in the US study would be higher than the CMV in the UK study. In both studies, each respondent provides the data on impulsivity scales and RScB (i.e., variables are being measured based on responses of a single source). Thus there is no reason to expect greater CMV in the replicated study from this source. There are differences in the recruited respondents (employees in the original UK study versus MTurk respondents in the USA replication study) and possibly in the survey administration method (unclear in the UK study versus online in the replication study). In future research, it may be worth exploring if either of these factors could explain possible differences in CMV across the two studies.

Social desirability bias (SDB) is another source of response bias that could result from the measurement method (i.e., bias resulting from self-reported scores). SDB refers to the under- or over-reporting of behaviors by respondents to appear more acceptable, or gain the approval of others (Aivazpour, Valecha, & Chakraborty, 2022; King & Bruner, 2000). With respect to self-report of risky security behaviors, SDB in responses is a distinct possibility. It may also be argued that respondents recruited from an employee pool are more likely to engage in socially desirable responding than anonymous respondents recruited via the online MTurk system. SDB would lead to self-reports of higher levels of compliance amongst those who comply less. No comparable bias is likely in the measurement of the dimensions of impulsivity. This would narrow the range of scores for RScB, but not that of impulsivity scores, leading to lower levels of correlation between impulsivity and RScB. Since SDB is likely to be higher in the employee pool of the original study, the correlations between RScB and impulsivity are likely to be lower in that pool than in the pool of anonymous MTurk respondents of the replication study.

We reiterate that the explanations offered for the differences in the levels of the correlations are somewhat speculative, and need empirical verification. Future studies should, in particular, focus on detecting the presence of common method variance, both from single source measurement bias and social desirability bias, and eliminating them when possible.

5 Exploration of the Data

The current study, along with that of Hadlington's research, and that of Egelman and Peer (2015a), provides a good starting point for the study of impulsivity in risky cybersecurity behaviors. However, there is potential for placing their research and consequently our current work on a more rigorous theoretical footing. The three studies base their work on an established and robust body of work for measuring impulsiveness. In contrast, the conceptualization of risky cybersecurity behavior as a theoretical construct is inadequate and needs further development. Currently, the risky cybersecurity behaviors scale appears to be a relevant, but a random collection of behaviors that introduce risk in disparate ways. For instance, using the same password for multiple accounts and disabling anti-virus software are both risky behaviors. However, they are not likely to be the result of the same causal variables, nor is it likely that they can be combated using the same techniques.

We conduct two forms of exploratory data analyses in a search of patterns: a factor analysis of survey participant responses and an examination of the correlations of each behavior with each of the three forms of impulsivity.

5.1 Factor Analysis in Search of a Typology

The objective of the exploratory factor analysis (EFA) was to discover the structure of RScB scale used in the study. The EFA method used was the principal axis factoring method with Promax rotation. We used eigen value greater than 1 as the extraction criteria. The results from the statistical analysis were as follows: Three factors emerged from our EFA (see Table 8). The three factors explain 74.5% of the total variance. While most of items load on factor one, items 3, 4 and 6 were loaded on a second factor, and, items 11 and 18 loaded on the third factor. One item, item 17, did not load onto any of the factors.

Table 8. Factor Analysis

Items	Factor1	Factor2	Factor3
1 Sharing passwords with friends and colleagues.	**0.955**	-0.119	-0.141
8 Downloading free anti-virus software from an unknown source.	**0.950**	-0.145	-0.039
9 Disabling the anti-virus on my work computer so that I can download information from websites.	**0.902**	-0.058	-0.053
16 Sending personal information to strangers over the Internet.	**0.900**	-0.11	0.027
15 Clicking on links contained in unsolicited emails from an unknown source.	**0.884**	-0.067	0.039
5 Entering payment information on websites that have no clear security information/certification	**0.838**	0.111	-0.16
19 Downloading data and material from websites on my work computer without checking its authenticity.	**0.833**	-0.028	0.055
12 Downloading digital media (music, films, games) from unlicensed sources	**0.616**	0.097	0.092
20 Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop)	**0.561**	0.105	0.091
10 Bringing in my own USB to work in order to transfer data onto it.	**0.491**	0.019	0.285
7 Relying on a trusted friend or colleague to advise you on aspects of online-security.	**0.680**	0.115	-0.01
14 Accepting friend requests on social media because you recognize the photo.	**0.586**	0.117	0.14
2 Using or creating passwords that are not very complicated (e.g. family name and date of birth).	**0.582**	0.214	-0.177
13 Sharing my current location on social media.	**0.446**	0.172	0.146
4 Using online storage systems to exchange and keep personal or sensitive information.	0.204	**0.501**	-0.015
3 Using the same password for multiple websites.	-0.137	**0.731**	-0.118
6 Using free-to-access public Wi-Fi.	0.09	**0.442**	0.134
11* Checking that software for your smartphone/tablet/laptop/PC is up-to-date.	0.198	-0.055	**-0.720**
18* Checking for updates to any anti-virus software you have installed.	-0.133	0.209	**-0.683**
×17 Clicking on links contained in an email from a trusted friend or work colleague.	0.057	0.282	0.346

*reverse coded; × item shows cross loadings on factors 2 and 3

We examined the statistical results to see if the items in each factor converged to an identifiable conceptual theme. Our principal finding in the factor analysis is that factors 1 and 2 do not exhibit conceptual convergence, but factor 3 does. The lack of conceptual convergence in factors 1 and 2 is inferred from two observations. First, each factor includes items that are not conceptually consistent. The activities in factor 1 included disparate issues (i.e., issues related to access control, downloading, and clicking on links). The activities in factor 2 included data storage, access control and network issues. Second, items that should logically fall under the same factor do not (i.e., two access control items load on factor 1 (Item 1: Sharing passwords with friends and colleagues, Item 2: Using or creating passwords that are not very complicated (e.g. family name and date of birth)) and one access control item loads onto factor 2 (Item 3: Using the same password for multiple websites). Thus, eighteen of the twenty items are not classified consistently in the exploratory factor analysis. The two items that load on factor 3 are planning-related items, helping us identify one conceptually consistent factor. In other words, there is conceptual convergence for only one of the three factors. Overall, the factor analysis is insufficiently helpful in clearly identifying the concepts underlying RScB. However, it can still shed some useful light in other ways.

From, an examination of the instructions given to the respondents, it appears more likely that each factor includes items that are performed at approximately the same frequency. The RScB scale asked

participants to state how often they had engaged in a particular unsafe cybersecurity activity during a previous six-month period. It was scored on a 7-point scale (0=never to 6=daily). Thus, it could be said that each factor includes activities that are performed at approximately the same frequency. The frequency with which an act is engaged in depends on how often the need or occasion to engage in that act arises and how likely it is that the user engages in that act.

The range of scores for all items is between 0 (never) and 6 (daily). We examined the medians because the distribution of the responses is skewed for each risky behavior item. Most activities in factor 1 have a median score of 0 (never) and some have a median score of 1 (once every three months). Overall, this indicates that users engage infrequently in the most risky activities. Despite the infrequency, there is considerable risk because every instance of rule transgression can result in substantial exposure or damage to information assets. One item in factor 2 (item 4) has a median score of 1 (once every three months) and two items (3 and 6) have a median of 3 (once a month). Item 4 (Using online storage systems to exchange and keep personal or sensitive information), which has a median score of 1, could be risky if the online storage systems are insecure, but the use of online storage services provided to employees by employer organizations or private services (e.g., Carbonite) available to individual customers are legitimate and secure ways to back up data. Thus, the frequency for this item may not be of concern or not dependent on the security of the system on which the information is stored. The other two items (3 and 6) which have median scores of 3 (once a month) seem to be more reflective of the frequency with which those acts have to be performed. For most users, creating passwords for websites is not a frequent occurrence. A median score of 3 (once a month) suggests that users may be re-using the same password for new websites may be common. A deeper examination of this issue may be warranted. The need to use public Wi-Fi (item 6) may arise for most users only when they are traveling because private Wi-Fi is usually available at work or at home.

The two items (11 and 18) in factor 3 both relate to updating software, which is a planned activity and is likely to be executed at pre-determined frequencies. The median score of 3 for both items is reflective of the frequency with which these acts have been scheduled to be performed.

By examining the data carefully, it is possible to determine which factors need to be addressed with the user in terms of reducing overall risk. Users appear to accept that some actions are risky and are more careful about not engaging in them. For instance, most users will encounter ‘links embedded in emails from unknown sources’ (item 15) almost on a daily basis. The frequency with which they click on such links has a median score of 0 (never), indicating that most users realize that clicking on embedded links is dangerous. On the other hand, users appear to be less convinced of the riskiness of other items, (e.g., ‘using same password for multiple websites’ (item 3)). The occasions for signing on to a new website are infrequent, and the median score of 3 (once a month) for this suggests that some users are using the same password almost every time they create a new account. This attitude of users needs to be addressed to avoid potential problems. Thus, individual behaviors have to be examined to determine user acknowledgement of the behavior as risky, and attention paid to those behaviors that the user has failed to accept as risky. We add the caveat that our statements are based on exploratory analysis of available data, and more rigorous data gathering is warranted before definitive conclusions are arrived at.

A second way of looking for qualitative patterns is to examine which dimensions of impulsivity individual items correlate to, if any. In the next section, we use this approach to look for such patterns.

5.2 Correlations of Impulsivity Dimensions to Individual Risky Security Behaviors

The objective of exploring the correlations of the impulsivity dimensions to the individual risky security behaviors was to identify if particular risky behaviors were more susceptible to a specific dimension of impulsivity. The results from the statistical analysis (i.e., the correlations of each item with each of the three dimensions of impulsivity are shown in Table 9) indicate that thirteen items (1, 2, 4, 5, 8, 9, 12, 13, 14, 15, 16, 19, 20) are significantly correlated to both motor and attentional impulsivities, five items (3, 6, 7, 10 and 17) are significantly correlated to motor impulsivity and two items (11 and 18) are correlated only to non-planning impulsivity. It should be noted that item 11 is correlated at $p<0.05$ level and item 18 is correlated only at $p<0.10$ level. It should also be noted that for all items, with the exceptions of items of 11 and 18, motor impulsivity is more highly correlated to the individual risky behavior than attentional impulsivity.

Table 9. Correlation Results of Risky Cybersecurity Behaviors and Impulsivity			
RScB items	**Attention**	**Motor**	**non planning**
1 Sharing passwords with friends and colleagues.	0.256***	0.566***	0.092
2 Using or creating passwords that are not very complicated (e.g. family name and date of birth).	0.186**	0.425***	0.06
3 Using the same password for multiple websites.	0.044	0.219**	0.034
4 Using online storage systems to exchange and keep personal or sensitive information.	0.222***	0.443***	0.072
5 Entering payment information on websites that have no clear security information/certification	0.217**	0.546***	0.065
6 Using free-to-access public Wi-Fi	0.113	0.24***	-0.01
7 Relying on a trusted friend or colleague to advise you on aspects of online-security.	0.093	0.441***	-0.024
8 Downloading free anti-virus software from an unknown source.	0.195***	0.501***	0.073
9 Disabling the anti-virus on my work computer so that I can download information from websites.	0.192**	0.539***	0.046
10 Bringing in my own USB to work in order to transfer data onto it.	0.031	0.364***	-0.071
11* Checking that software for your smartphone/tablet/laptop/PC is up-to-date.	0.12	-0.015	0.167**
12 Downloading digital media (music, films, games) from unlicensed sources	0.166**	0.45***	0.007
13 Sharing my current location on social media.	0.126**	0.441***	0.074
14 Accepting friend requests on social media because you recognize the photo.	0.128**	0.469***	0.023
15 Clicking on links contained in unsolicited emails from an unknown source.	0.131**	0.575***	0.02
16 Sending personal information to strangers over the Internet.	0.191**	0.559***	0.08
17 Clicking on links contained in an email from a trusted friend or work colleague.	0.05	0.285***	-0.026
18* Checking for updates to any anti-virus software you have installed.	0.082	-0.123	0.115^
19 Downloading data and material from websites on my work computer without checking its authenticity.	0.149**	0.6***	0.105
20 Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop)	0.152**	0.436***	-0.008
**p<0.01; * p<0.05; ^ marginal significance			

The salient finding is that neither the thirteen items that are correlated to both motor and attentional impulsivities, nor the five items correlated to motor impulsivity alone show a clear underlying conceptual theme. Also, the two items correlated only to non-planning impulsivity (items 11 and 18) relate to actions – checking for updates – that can be planned ahead of time, scheduled, and executed, and thus their correlation to non-planning impulsivity is consistent with expectations.

An alternate way of viewing the correlations of the eighteen items (the twenty items excluding planning-related items 11 and 18) would be to say that the correlation to motor impulsivity is higher than the correlation to attentional impulsivity. These items refer to activities that are not planned ahead of time for execution at a particular point in time. A user may resolve not to engage in an activity (e.g., he/she may resolve not to use the same password for two accounts) but such resolutions are likely to be violated if the need to create a new password comes up unexpectedly. A user is likely to create the password on the spur of the moment, possibly contravening prior resolutions about rules to follow. Such spur-of-the-moment actions are reflective of motor impulsivity. An examination of each of the items correlating significantly to motor impulsivity indicates that they are all susceptible to spur-of-the-moment actions.

The RScB items that are significantly correlated to attentional impulsivity are subject to uncertainty about the decision or a lack of focus, consistent with the definition of attentional impulsivity. An example of a decision that may produce uncertainty – the decision of whether to share a password with a friend or colleague may produce a conflict (i.e., the rule stating that one should not share passwords may conflict with the normal desire of people to be cooperative with and trusting of friends). Those who score high on attentional impulsivity are likely to succumb to the more ingrained and automated response to cooperate with friends and colleagues in the face of conflicting choices. The lack of focus may be due to attempts to

multi-task or due to external distractions. An example of actions that are likely to be susceptible to a lack of focus would be 'sharing current location on social media'. For this example, it is easier to accept that the act may be performed in a moment of distraction. In effect, those who score higher on attentional impulsivity are more likely to do it. In a similar vein, a common-sense explanation can be provided for other items that correlate significantly with attentional impulsivity. What is more challenging is to understand why some items did not correlate with attentional impulsivity. For example, clicking on a link embedded in an email from a trusted source (item 17) does not correlate with attentional impulsivity. At a common-sense level, one could argue that one is more likely to engage in this when one is distracted. Thus, it is difficult to explain the absence of a significant correlation between this item and attentional impulsivity.

In general, explanations of behavior based on variations of individual characteristics provide an understanding of the behavior but are difficult to use in the development of solutions to problems of security. One approach is to circumvent the role of individual characteristics (i.e., automate actions that have to be taken, such as updates of software). Automated systems can be rigid and may curtail user discretion or preferences. The other approach is to raise awareness of the role of the individual characteristics among users and provide training to compensate for the individual differences. The effectiveness of training remains to be demonstrated.

In the current context of the effects of impulsivity, some activities, such as updating software, can be planned. Users with higher non-planning impulsivity may still fail to execute. This can be compensated for by automating the process. In other words, the effects of non-planning impulsivity can be compensated for. Risky behaviors which are highly correlated to motor and attentional impulsivities are more difficult to curb. Automation can be tried but is likely to lead to other problems. For instance, it may be possible to use system generated passwords instead of user generated passwords, but this is likely to result in users having a difficult time remembering passwords. Training may provide a starting point to encourage and teach users to avoid common pitfalls, but has its limitations. For instance, users may be instructed to use different passwords for different accounts, but as the number of accounts that each user has proliferates, the user is likely to surrender to using a few passwords to facilitate remembering the passwords.
In effect, the relationship between impulsivity and risky security behaviors highlights one of the reasons why cybersecurity remains intractable.

6 Conclusion

Our primary goal was to replicate the Hadlington (2017) study on the influence of impulsivity on risky cybersecurity behavior and to explore the data in search of additional insights. Our replication shows that the results of the original study are mostly robust. It also increases confidence in the Abbreviated Barratt Impulsivity Scale (Coutlee et al., 2014) and in the explanatory potential of impulsivity on risky cybersecurity behaviors. It is evident that there is much scope for research on the effects of impulsivity in the area of cybersecurity behaviors. Hadlington's article provides the initial empirical basis for a relationship between impulsivity and risky cybersecurity behavior and the replication bolsters the support for the existence of linkage.

A cursory examination is sufficient to indicate the need for a more rigorous conceptualization of the construct, risky cybersecurity behavior. Exploratory factor analysis produced three factors, each of which is reflective of the frequency with which users perform those acts. However, this does not provide conceptual clarity of risky cybersecurity behavior, nor does it enhance our understanding of the role of impulsivity. However, a review of responses to individual items is helpful in understanding user perception of what they consider risky. An examination of the correlations of each item with each of the three dimensions of impulsivity provides some useful insight. It indicates that actions that can be planned, i.e., a specific time set for them, such as updating software, are susceptible to non-planning impulsivity. Other actions, usually actions from which the user should refrain, are difficult to plan, i.e., the occasions when they need to be (not) performed appear somewhat randomly, and during the course of other activities. Such actions may be performed spontaneously despite any prior resolve by users not to engage in them. They are susceptible primarily to motor impulsivity, and to a much lesser extent to attentional impulsivity. The exploratory analysis with correlations of impulsivity with each item clearly shows that motor impulsivity is the most important dimension in disinhibiting user behavior with respect to engaging in unsafe actions.

In sum, we have confirmed that the personality characteristic impulsivity is highly correlated to risky cybersecurity behaviors, and is therefore important in understanding the behaviors. Additionally, we have provided preliminary empirical evidence for the possible influence of different dimensions of impulsivity on different risky cybersecurity behaviors. Further research needs to be done to develop a theory-based conceptual structure for risky cybersecurity behaviors before undertaking to develop a theoretical model of the relationship between impulsivity and risky cybersecurity behaviors.

Acknowledgments

We would like to thank the senior editor and the reviewers for their constructive comments. This manuscript has greatly benefited from their feedback.

References

Aivazpour, Z., Valecha, R., & Chakraborty, R. (2022). Data breaches: An empirical study of the effect of monitoring services. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 53(4), 65-82.

Aurigemma, S., & Mattson, T. (2019). Effect of long-term orientation on voluntary security actions. *Information & Computer Security*.

Borgatta, E. E (1964). The structure of personality characteristics. *Behavioral Science*, 9, 8-17.

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. arXiv preprint: arXiv:1606.00887.

Chamberlain, S. R., Lust, K., & Grant, J. E. (2020). Cocaine use in university students: Relationships with demographics, mental health, risky sexual practices, and trait impulsivity. *CNS Spectrums*, 1-8

Coutlee, C. G., Politzer, C. S., Hoyle, & R. H., Huettel, S. (2014). An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the Barratt Impulsiveness Scale Version 11. *Archives of Scientific Psychology*, (2), 1–12.

D'Arcy, J., Herath, T., Yim, M.-S., Kichan, N. & Raghav, H.R. (2018). Employee moral disengagement in response to stressful information security requirements: A methodological replication of a coping-based model. *AIS Transactions on Replication Research*, 4(8), 1-17 .

Davis, R. A., Flett, G. L., & Besser, A. (2002). Validation of a new scale for measuring problematic internet use: Implications for pre-employment screening. *Cyberpsychology & Behavior*, 5(4), 331–345.

Dennis, A. R., & Valacich, J. S. (2014). A replication manifesto. *AIS Transactions on Replication Research*, 1(1), 1-5.

Egelman, S., & Peer, E. (2015a). Predicting privacy and security attitudes. *Computers & Society*: *The Newletter of ACM SIGCAS*, 45(1), 22–28.

Egelman, S., & Peer, E. (2015b). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems (pp. 2873–2882).

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cybersecurity behavior intentions. *Computers & Security*, (73), 345-358.

Hadlington, L. (2017). Human factors in cybersecurity; Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon,* (3), 1-18.

Hofstede, G. (1980). Culture's consequences: International differences in work related values. Beverly Hills, CA: Sage.

Hogarth, L, Chase, H. W., and Baess, K. (2012). Impaired goal-directed behavioral control in human impulsivity. *Quarterly Journal of Experimental Psychology,* 65(2), 305-16.

Jakubczyk, A., Klimkiewicz, A., Mika, K., Bugaj, M., Konopa, A., Podgórska, A., & Wojnar, M. (2013). Psychosocial predictors of impulsivity in alcohol-dependent patients. *The Journal of Nervous and Mental Disease*, 201(1), 43.

Keil, M., Tan, B. C., Wei, K. K., Saarinen, T., Tuunainen, V., & Wassenaar, A. (2000). A cross-cultural study on escalation of commitment behavior in software projects. *MIS Quarterly*, 24(2), 299-325.

Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology*, 11, 3030.

King, M. F. & Bruner, G. C. (2000). Social desirability bias: A neglected aspect of validity testing. *Psychology & Marketing*, 17(2), 79-103.

Langewisch, M. W. J. & Frisch, G. R. (1998). Gambling behavior and pathology in relation to impulsivity, sensation seeking and risky behavior in male college students. *Journal of Gambling Studies,* (14), 245-262.

Maasberg, M., Warren, J., & Beebe, N. L. (2015). The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits. In Proceedings of 48th Hawaii International Conference on System Sciences. IEEE.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151-156.

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.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879.

Ryb, G.E., Dischinger, P.C., Kufera, J.A., & Read, K.M. (2006). Risk perception and impulsivity: Association with risky behaviors and substance abuse disorders. *Accident Analysis and Prevention,* 38(3), 567-573.

Shropshire, J., Warkentin, M., Johnston, A. C., & Schmidt, M.B. (2006). Personality and IT security: An application of the five-factor model. *Americas Conference on Information Systems (AMCIS),* 3443–3449.

Suresh, K. P., & S. Chandrashekara. (2012). Sample size estimation and power analysis for clinical research studies. *Journal of Human Reproductive Sciences*, 5(1).

Winters, K.C., Botzet, A.M., Fahnhorst, T., Baumel, L., and Lee, S. (2009). Impulsivity and its relationship to risky sexual behaviors and drug abuse. *Journal of Child & Adolescent Substance Abuse,* 18(1), 43-56.

Appendix A: Measurement Items

Table A1. Measurement Items

Items	Construct
1 Sharing passwords with friends and colleagues. 2 Using or creating passwords that are not very complicated (e.g. family name and date of birth). 3 Using the same password for multiple websites. 4 Using online storage systems to exchange and keep personal or sensitive information. 5 Entering payment information on websites that have no clear security information/certification. 6 Using free-to-access public Wi-Fi. 7 Relying on a trusted friend or colleague to advise you on aspects of online-security. 8 Downloading free anti-virus software from an unknown source. 9 Disabling the anti-virus on my work computer so that I can download information from websites. 10 Bringing in my own USB to work in order to transfer data onto it. 11* Checking that software for your smartphone/tablet/laptop/PC is up-to-date. 12 Downloading digital media (music, films, games) from unlicensed sources 13 Sharing my current location on social media. 14 Accepting friend requests on social media because you recognize the photo. 15 Clicking on links contained in unsolicited emails from an unknown source. 16 Sending personal information to strangers over the Internet. 17 Clicking on links contained in an email from a trusted friend or work colleague. 18* Checking for updates to any anti-virus software you have installed. 19 Downloading data and material from websites on my work computer without checking its authenticity. 20 Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop).	Risky Cybersecurity Behaviors (RScB)
Attention 1. I don't "pay attention." 2. I am self-controlled. 3. I concentrate easily. 4. I am a careful thinker. 5. I am a steady thinker. *Motor* 6. I do things without thinking. 7. I say things without thinking. 8. I act "on impulse". 9. I act on the spur of the moment. *Non planning* 10. I plan tasks carefully. 11. I plan trips well ahead of time. 12. I plan for job security. 13. I am future oriented.	Impulsivity
1 I think that management have the responsibility to ensure a company is protected from cybercrime. 2* I am aware of my role in keeping the company protected from potential cybercriminals. 3 I believe everyone in the company has a role to play in protecting against threats from cybercriminals. 4 It is hard to know how I can help protect the organization from cybercrime. 5 I don't have the right skills to be able to protect the organization from cybercrime. 6 I do not feel that IT security is a priority within my organization. 7 Computer systems provide all the protection a company needs. 8 I think that reporting cybercrime is a waste of time. 9 The police lack the capacity to deal with cybercrime effectively. 10 I believe that cybercriminals are more advanced than the people who are supposed to be protecting us. 11 I think that information provided by the government and police on cybercrime is not relevant to businesses. 12 I feel that the police are far too busy to deal with cybercrime. 13 I worry that if I report a cyberattack to the police it might damage the reputation of the company 14* I think more could be done to communicate the risks from cybercrime to individuals in the organization. 15* I am aware of the company's IT use policy and attempt to follow it. 16 I would not know how to report a cyberattack if one happened. 17 I don't think that reporting a cyberattack on the company is my responsibility.	Attitudes toward cybersecurity and cybercrime

Table A1. Measurement Items	
18 I don't pay attention to company material about the threats from cybercrime. 19* I am confident that I would be able to spot the signs of a cyberattack. 20* I think the biggest threat for IT systems comes from people within the company. 21* I feel that any individual within the company are at risk of manipulation from confidence tricksters. 22 I think that cyber criminals only target a company when there is a substantial financial gain. 23 I believe only large companies are targeted by hackers and cybercriminals. 24 I feel that only companies that take payments using online systems are at risk of being victims of cybercrime. 25 I don't think I know who is responsible for protecting the company from cybercrime.	
I am most comfortable online. I feel safest when I am on the internet. You can get to know a person better on the internet than in person. I often find it peaceful to be online. I can be myself online. I get more respect online than "in real life". People accept me for who I am online. Online relationships can be more fulfilling than offline. I am at my best when I am online. I wish my friends and family know how people regard me online. The internet is more "real" than real life. I say or do things on the internet that I can never do online. When I am online I can be carefree. Few people love me other than those I know online. I am less lonely when I am online. I cannot see myself ever without the internet for too long. The internet is an important part of my life. I feel helpless when I don't have access to the internet. I am bothered by my inability to stop using internet so much. I often keep thinking about something I experienced online well after I have logged off. When I am on the internet I often feel a kind of "rush" or emotional high. I use the internet more than I ought to. People complain that I use the internet too much. I never stay no longer than I had planned. When I am not online I often think about the internet. The offline world is less exciting than what I can do online. I can't stop thinking about the internet. Even though there are times that I would like to, I can't cut down on my use of the internet. My use of the internet sometimes seems beyond my control. When I am online I don't think about my responsibilities. When I have nothing better to do, I go online. I find that I go online more when I have something else I am supposed to do. When I am online I don't need to think about offline problems. I sometimes use the internet to procrastinate. I often use the internet to avoid doing unpleasant things. Using the internet is a way to forget about the things I must do but don't really want to do.	OCS (Internet addiction)

About the Authors

Zahra Aivazpour is an Assistant Professor at California Polytechnic State University, San Luis Obispo. Her publications appeared in IS journals including *the DATABASE for Advances in Information Systems* and in the proceedings of conferences such as *American Conference on Information Systems, International Conference on Information Systems,* and *Hawaii International Conference on System Sciences*. Her research interests lie in the areas of cybersecurity, privacy and data analytics.

V. Srinivasan (Chino) Rao is a Professor Emeritus at the University of Texas at San Antonio. He obtained his Ph.D. from the University of Texas at Austin. His research is currently limited to guiding current and past doctoral students in their projects. He has published in leading academic journals, such as *MIS Quarterly, Management Science, Communications of the Association for Information Systems* and *Group Decision and Negotiation.*