The Journal of the Southern Association for Information Systems

Volume 7 | Issue 1 Article 2

September 2020

Risk and Demographics' Influence on Security Behavior Intentions

Ramakrishna Ayyagari
University of Massachusetts Boston, r.ayyagari@umb.edu

Austin Crowell
austincrowell1@gmail.com

RISK AND DEMOGRAPHICS' INFLUENCE ON SECURITY BEHAVIOR INTENTIONS

Ramakrishna Ayyagari
University of Massachusetts Boston
r.ayyagari@umb.edu

Austin Crowell
University of Massachusetts Boston
austincrowell1@gmail.com

ABSTRACT

Behavioral information security has become an important aspect of information security. In this study, we extend previous works on developing a comprehensive tool to measure security behaviors (i.e. Security Behavior Intentions scale – SeBIS (Egelman and Peer, 2015)). We extend the work on SeBIS by 1) proposing the use of security domain-specific risk as opposed to a generic risk measure, 2) investigating differences in SeBIS across age, gender, education and experience, and 3) providing suggestions for improving SeBIS measures. Survey results from our study provide support for security risk - device securement relationship, a previously unsupported link. We also uncover the role of demographics in influencing SeBIS. Overall, our study contributes to, and further establishes SeBIS as a predictive tool for measuring security behaviors.

Keywords

Security Behaviors, SeBIS, Risk, Individual Differences, Awareness

INTRODUCTION

In recent times, considerable emphasis is placed on the 'human element' in information security. End-users are argued to be the weakest link in security chain (Mitnick, 2003; Yan et al., 2018), enablers of cyberattacks (OTA, 2018), and most of them don't follow security best practices (Pew Research Center, 2017). Accordingly, research has studied various behavioral aspects of information security. These include: compliance behaviors (Aurigemma and Mattson, 2017; Siponen and Vance, 2010), secure email behavior (Ng, Kankanhalli, and Xu, 2009), omissive behaviors (Workman, Bommer, and Straub, 2008), and protective behaviors (Chen and Li, 2017; Liang and Xue, 2010). In accordance with their research emphasis, most of these behavioral studies focus on a particular behavior – e.g. email behavior (Ng et al., 2009) or antispyware usage behavior (Liang and Xue, 2010).

As is evident from above studies, security behaviors are wide-ranging. Rather than focus on one particular security behavior, some researchers study how to capture security behaviors that span wide-range of information security behaviors. Here, researchers are interested in developing a security behavior scale that has broader application rather than to a specific purpose. Previous attempts to capture wide-ranging security behaviors included developing a taxonomy of security behaviors (Stanton, Stam, Mastrangelo, and Jolton, 2005), and developing measures for security scales.

We could identify two recently developed 'holistic' security behavior scales in the literature. Human Aspects of Information Security – Questionnaire (HAIS-Q) (Parsons, McCormac, Butavicius, Pattinson, and Jerram, 2014) and Security Behavior Intentions Scale (SeBIS) (Egelman and Peer, 2015). HAIS-Q is an awareness scale and includes behaviors. It uses a knowledge-attitude-behavior model to develop the scale. In other words, HAIS-Q measures knowledge, attitude and behavior. On the other hand, SeBIS scale specifically focuses on behaviors and is much more parsimonious. Since they both measure security behavior, there is conceptual overlap between HAIS-Q and SeBIS scales. For example, some of the dimensions they measure include internet usage and passwords behaviors. HAIS-Q scale is validated in various studies and exhibits good properties (McCormac et al., 2017; Parsons et al., 2017; Parsons et al., 2014), whereas SeBIS scale has marginal properties and previous studies that used SeBIS found issues with

reliabilities. Previous research has called for further testing of SeBIS scale (Egelman and Peer, 2015; Gratian, Bandi, Cukier, Dykstra, and Ginther, 2018). To advance security research, validated measures of security behavior intentions are needed (Thompson, McGill, and Wang, 2017).

Therefore, in this research we provide a further test for SeBIS scale. Previous studies of SeBIS scale also included the impact of demographics and risk on security behaviors. In this study, we argue and provide support for a security domain-specific risk awareness scale. In addition, we test the impact of demographic variables on SeBIS scales.

In summary, we make the following contributions:

- We further validate the SeBIS scale and propose modifications to SeBIS scale
- We argue for, and provide support for the use of security domain-specific risk scale in studying security behaviors
- Impact of demographic variables such as age, gender, education and experience is established

The rest of the paper is organized as follows. First, we provide literature review on behavioral security studies (including previous SeBIS studies) and propose our hypotheses. Next, we discuss the research methodology used and present the results. Finally, we conclude by discussing the results and implications from our study.

BACKGROUND AND HYPOTHESES

Behavioral Intentions in IS and Information Security Literature

One of the mature streams of IS research is the adoption and use of IT (Tamilmani, Rana, and Dwivedi, 2020; Venkatesh, Morris, Davis, and Davis, 2003). Since implementation of new technology is costly and potentially disastrous, a major stream of research focused on adoption and use of IT (Venkatesh et al., 2003). Individuals have to utilize the technology or it will be a wasted investment for organizations (Berns, 2017). Researchers have used various theories to explain individual adoption and use of IT. Some of the widely used theories are Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Theory of Planned Behavior (TPB) and Unified Theory of Acceptance and Use of Technology (UTAUT) (Tamilmani et al., 2020; Venkatesh et al., 2003). A recurring theme in these models is the use of behavioral intentions of use as a surrogate for actual use.

Over the decades, the IS research has used behavioral intentions as a variable of interest in various contexts such as online healthcare, cloud computing, mobile banking etc. (Luarn and Lin, 2005; Shiau and Chau, 2016; Swar, Hameed, and Reychav, 2017). The study of behavioral intentions has carried over to the information security research also (Cram, D'arcy, and Proudfoot, 2019; Trang and Brendel, 2019). Behavioral intentions in security research can be broadly classified into pro-security or anti-security behaviors (Jaeger, 2018). Pro-security behaviors reflect intentions that are supportive of information security. These can be in terms of complying with security policies, using security tools and technologies (Chen and Li, 2017; Liang and Xue, 2010). Anti-security behaviors reflect intentions that are disruptive of information security. These can be in terms of violating security policies, not following security requirements and, intentions towards unethical IT use (Chatterjee, Sarker, and Valacich, 2015). As indicated in the Introduction section, we further study the security intentions at a holistic level by extending the SeBIS scale.

SeBIS Related Literature

To develop a predictive tool that could be used to measure security behaviors, Egelman and Peer (2015) developed the SeBIS scale. The scale is derived based on best practices prescribed by the United States Computer Readiness and Security Team (US-CERT), internet service providers, industry experts, among others. After extensive testing, four dimensions of security behaviors are proposed. These are device securement, password generation, proactive awareness and updating. Device Securement focuses on security behaviors such as use of PIN on phones used to protect access. Password Generation focuses on

good password behaviors such as using strong passwords and not reusing passwords. Proactive Awareness focuses on users' security awareness such as identifying valid web links. Finally, Updating focuses on users' behavior with applying software patches. Further description of these four factors is presented in Table 1.

Dimensions of SeBIS scale	Description
Device Securement	This dimension refers to users' behaviors in logically securing their devices. Themes covered in this area involve screen locks using PIN/Passwords, locking devices when stepping away from devices, among others.
Password Generation	This dimension refers to users' behaviors concerning password hygiene. Themes covered in this area involve using strong passwords, not reusing passwords, among others.
Proactive Awareness	This dimension focuses on users' awareness in reading contextual cues. Themes covered in this area involve whether users notice web links, among others.
Updating	This dimension focuses on users' behaviors with patching vulnerabilities. Themes covered in this area involve whether users update programs when prompted, among others.

Table 1: SeBIS scale dimensions

SeBIS research is still in the nascent stage and mixed results are reported from the use of SeBIS in Behavioral Information Security research. Table 2 summarizes previous SeBIS studies and their key findings in the context of this study. A recurring theme in these studies tested the relationship between risk-taking perceptions and SeBIS scale dimensions. In these studies, Domain-Specific Risk-Taking (DOSPERT) scale is used to measure risk-taking propensity (Egelman and Peer, 2015; Gratian et al., 2018). The DOSPERT scale consists a total of 30 items in different risk domains such as health/safety, recreational, financial, ethical and social (Blais and Weber, 2006). The premise for developing DOSPERT scale is that risk taking in one domain doesn't translate to other domains (Blais and Weber, 2006; Szrek, Chao, Ramlagan, and Peltzer, 2012). For example, high recreational risk takers do not exhibit the same risk-taking propensity in financial domain (Hanoch, Johnson, and Wilke, 2006).

Mixed results are reported with dimensions of risk in SeBIS studies. For example, social risk-taking perceptions are significantly related to password generation security behaviors in Egelman and Peer (2015), however they are unrelated in Gratian et al. (2018). Because of the newness of SeBIS scale and mixed findings, further testing of SeBIS scale is suggested. Our study addresses this call and contributes in the establishment of a holistic security behavior scale

Study	Key Findings related to SeBIS	Potential issues/ suggestions for future work
Egelman and Peer (2015)	Developed a parsimonious SeBIS scale consisting of four factors Reliabilities range in 0.6-0.7 Mixed correlations with risk scale	Further testing of SeBIS scales is needed
Egelman, Harbach, and Peer (2016)	SeBIS scale is a good predictor for actual security behaviors	Potential of SeBIS as a predictive tool, further testing needed

	Reliabilities for SeBIS factors range in 0.6-0.7	
Gratian et al. (2018)	Validates and extends Egelman and Peer (2015)'s study. Individual differences exist in security behavior intentions	Weaker reliabilities for SeBIS scale reported (0.6 to 0.75) Relation between risk and security behaviors are mixed Further testing of SeBIS scale is suggested
Wash, Rader, and Fennell (2017)	SeBIS scale is not used in its entirety	-
Tischer et al. (2016)	Users do plug-in USB drives they find	SeBIS scale reliabilities are much lower, ranging from 0.4-0.7

Table 2: Summary of previous SeBIS studies

Further, although DOSPERT covers different domains, information security risk does not fit in any of the DOSPERT domains (i.e. health/safety, recreational, financial, ethical and social). Some of the items used in these domains are "Going camping in the wilderness (Recreational)", "Passing off somebody else's work as your own (Ethical)", "Sunbathing without sunscreen (health/safety)" (Blais and Weber, 2006). We believe these items and domains do not capture the Information Security risks. Therefore, we propose and use a security risk scale that is more specific to information security.

In behavioral information security research, risk perceptions are measured in at least couple of different, but related ways. One method is to measure risk by measuring the components that create risk. Since risk is described as a combination of severity of a threat and the susceptibility of a resource, risk perceptions are measured as two constructs - severity and susceptibility (Johnston and Warkentin, 2010; Liang and Xue, 2010). A more parsimonious way of measuring risk perception is to directly measure risk using a single construct (Guo, Yuan, Archer, and Connelly, 2011). (Guo et al., 2011)'s risk perception scale consists of only three items. A sample item for our context is "Not having a passcode on my devices can put important data at risk". The risk perceptions measured by Guo et al. (2011) performed as well as other risk scales that used two measures (i.e. severity and susceptibility) (Vance, Brinton Anderson, Brock Kirwan, and Eargle, 2014). Further, Guo et al. (2011)'s risk perceptions measures are well established and also used in various contexts (Haag and Eckhardt, 2014). Therefore, use security risk scale adapted from Guo et al. (2011). The scale measures users' perception of risk associated with a particular security behavior. We believe this is an appropriate security risk measure because SeBIS measures security behavior intentions.

Hypotheses

Risk: Understanding how users perceive risks enables us to understand users' behaviors. For example, Health Belief Model argued that if individuals perceive a behavior as risky, they would choose a behavior that is less risky (Becker, 1974). Accordingly, previous security research has tested the link between risk perceptions and behavioral intentions (Liang and Xue, 2010; Ng et al., 2009; Workman et al., 2008). Previous research on SeBIS has also tested the relationship between risk perceptions and security behaviors (Egelman and Peer, 2015; Gratian et al., 2018). Therefore, we hypothesize

H1: Individuals' risk perceptions will be significantly related to their security behavior intentions.

Specifically,

H1a-d: Individuals' (device securement, password generation, proactive awareness, and updating) risk perceptions will be significantly related to their (device securement, password generation, proactive awareness, and updating) intentions.

Demographic variables: Gender studies have shown that women and men differ in their risk-taking propensities. Women are inclined to take fewer risks in various domains (Harris, Jenkins, and Glaser, 2006). In shopping context, women perceive higher risk while shopping online (Garbarino and Strahilevitz, 2004). Also, risk taking behaviors are shown to vary by age (Rolison, Hanoch, Wood, and Liu, 2014).Further, inexperienced people are known to take more risks (Menkhoff, Schmidt, and Brozynski, 2006). Previously, age, gender and education are proposed to influence security behavior intentions (Herath and Rao, 2009). Demographic variables such as age, gender are known to influence strength of security behaviors (McCormac et al., 2017; Sheng, Holbrook, Kumaraguru, Cranor, and Downs, 2010). Therefore, we hypothesize

H2: Individuals' (device securement, password generation, proactive awareness, and updating) intentions will vary across gender, education, experience and age.

METHODOLOGY

Similar to previous SeBIS studies, we have used a survey methodology. As explained previously, one key difference in our study is the use of risk scale. The items used in this study are presented in Table 3.

Concept Measured and Related Items[1]	
SeBIS -Updating	• When I'm prompted about a software update, I install it right away. *(Updating)* • I try to make sure that the programs I use are up-to-date. *(Updating)* • I verify that my anti-virus software has been regularly updating itself. *(Updating)*
SeBIS – Device Securement	• I manually lock my computer screen when I step away from it. *(Device Securement)* • I set my computer screen to automatically lock if I don't use it for a prolonged period of time. *(Device Securement)* • I use a PIN or passcode to unlock my mobile phone. *(Device Securement)* • I use a password/passcode to unlock my laptop or tablet. *(Device Securement)*
SeBIS – Proactive Awareness	• I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon). *(Proactive Awareness)* • If I discover a security problem, I continue what I was doing because I assume someone else will fix it. *(Proactive Awareness)* • When someone sends me a link, I open it without first verifying where it goes. *(Proactive Awareness)* • When browsing websites, I mouse over links to see where they go, before clicking them. *(Proactive Awareness)* • I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar. *(Proactive Awareness)*
SeBIS – Password Generation	• I do not change my passwords, unless I have to. *(Password Generation)* • I use different passwords for different accounts that I have. *(Password Generation)* • I do not include special characters in my password if it's not required. *(Password Generation)*

[1] SeBIS Items from Egelman and Peer (2015), 5-point Likert scale (Never to Always). Risk Items from (Guo et al., 2011), 5-point Likert scale (Strongly Disagree to Strongly Agree)

	• When I create a new online account, I try to use a password that goes beyond the site's minimum requirements. *(Password Generation)*
Risk	The anchor question is changed to measure risk perceptions for different SeBIS domains (i.e. 'Reusing the same password' for Password Generation or 'Not updating software' for Updating or 'Not checking the URL bar for the lock icon or "https://":' for Proactive Awareness) Risk measure for Device Securement Not having a passcode on my devices: • Can cause damages to computer security. • Can put important data at risk. • Will most likely cause security breaches.

Table 3: Concepts Measured and Related Items

A web survey with items for SeBIS, risk scales, and demographic variables was created using Qualtrics. A link for the survey was sent to the University's research recruitment email service. This service is provided by the authors' university. In essence, a sample of university students is recruited to participate in research studies. The link to our survey was sent to a random sample from this group. The participation in the study was optional and no incentive was given to participate in this study (monetary or extra-credit for courses). A total of 209 responses were received. After dropping responses with incomplete data, 163 data points remained.

RESULTS

We have used SPSS® for statistical analysis. Table 4 shows the descriptive statistics of the respondents. The sample was almost equally split on gender (53.4% female). Since our study was conducted at a large university, majority of respondents were young, undergraduate students. Further, computer/Internet experience was captured using a qualitative self-rating and 41.7% of the respondents consider themselves to be in the advanced and expert category.

Demographics	
Gender	53.4% Female
Age	18-24 Years – 53.4% 25-34 years – 23.3% >35 years – 23.3%
Education	Undergraduate – 70.6% Graduate – 29.4%
Experience	Advanced/Expert – 41.7%

Table 4: Descriptive statistics

Before testing the hypotheses, we tested the validity of SeBIS and Risk measures. We used the same 16-item SeBIS scale as is used in the previous research (Egelman and Peer, 2015; Gratian et al., 2018). Our initial factor analysis of 16-item SeBIS scale yielded a five-factor model as shown in Table A1, Appendix A. This is different from the original four-factor solution.

A close inspection of 5-factor solution suggested two potential problems. The device securement item 'I use a PIN or passcode to unlock my mobile phone' (SeBIS5ssSEC) loaded highly on Factor 5. Since the

conceptualization of SeBIS scale (in 2014), the biometric approach for authentication has grown rapidly (Biometrics-today, 2017). For example, first major phone with biometrics was released in 2013 (Agomuoh, 2017) and it is expected that by 2020, 100% of smartphones will have biometric capabilities (Biometrics-today, 2016). Given this growth, it is not surprising that users are more comfortable using biometric technologies for authentication (IBM, 2018). Therefore, we argue that the context for Device Securement item 'I use a PIN or passcode to unlock my mobile phone' is outdated. Methodologically, this item did not load with other Device Securement items either (as shown in Table A1, Appendix A). Accordingly, we have dropped this item from further analysis.

Further, a construct scale's dimensionality can be impacted if the scale consists of reverse-coded items (Herche and Engelland, 1996). Out of five 'proactive awareness' scale items, the item 'When browsing websites, I mouse over links to see where they go, before clicking them' is reverse-coded compared to other 'proactive awareness' items (as listed in Table 3). Therefore, this item is dropped from further analysis. Even after dropping these two items, each of the SeBIS dimensions have at least three items (Raubenheimer, 2004). Subsequent factor analysis yielded a four-factor solution for SeBIS items as shown in Table A2 in Appendix A.

Next, we used Cronbach's alpha (α) to measure reliability of the scales. The results indicated that SeBIS and risk scales exhibited moderate to very good reliabilities (Hinton, McMurray, and Brownlow, 2004). Specifically, α(SeBIS-updating) is 0.75, α(SeBIS-device securement) is 0.65, α(SeBIS-proactive awareness) is 0.63, α(SeBIS-password generation) is 0.67 and α(risk) ranged from 0.85 to 0.94. The above reliabilities for SeBIS scales are generally better than previously reported (Gratian et al., 2018; Tischer et al., 2016).

	Securement	Passwords	Awareness	Updating
Risk	0.24**	0.32**	0.25**	0.39**

Table 5: Standardized regression coefficients. **p<0.01

Table 5 shows the regression coefficients on factor scores of risk and SeBIS dimensions. Hypothesis H1 proposed that individuals' risk perceptions would be significantly related to their security behavior intentions. The standardized coefficients ranged from 0.24 to 0.39, with the strongest relationship for SeBIS (updating) dimension. These results support H1a-d.

	Securement	Passwords	Awareness	Updating
Age		1.61^{+}	2.32*	
Gender		1.90*		3.11**
Education			1.38^{+}	
Experience			1.74*	2.45**

Table 6: t-test for mean differences for SeBIS dimensions. **p<0.01; *p<0.05, $^{+}$p<0.1

Hypothesis H2 proposed that SeBIS dimensions would vary across gender, education, experience and age. Table 6 shows the mean differences for SeBIS dimensions for gender, education, experience and age. The results indicate that significant differences for age were found for password generation ($t=1.61$, $p<0.1$) and proactive awareness ($t=2.32$, $p<.05$). Gender differences were also found for password generation ($t=1.90$, $p<0.05$) and updating ($t=3.11$, $p<0.01$) dimensions. Only difference for education was found for proactive

awareness ($t=1.38$, $p<0.1$). Experience made a difference for proactive awareness ($t=1.74$, $p<0.05$) and updating ($t=2.45$, $p<0.01$). These results provide partial support for H2.

DISCUSSION

Before discussing the contributions, we point out the limitations of this study. We have used behavior intentions rather than actual behaviors. Although there is evidence that intentions reflect actual behavior (Egelman et al., 2016), future studies can incorporate actual behaviors. Further, although we have taken precautions like providing confidentiality and anonymity to respondents, we still acknowledge the limitation of self-reports. In addition, since the respondents came from a University, it is likely that the respondents have different educational background than general population. As with other research studies, we had to deal with dropped responses from our sample. Therefore, further testing with different populations will help generalize the SeBIS scale.

Previous SeBIS research that tested the relationship between risk (measured using DOSPERT scale) and SeBIS dimensions found mixed results. For example, Gratian et al. (2018) found significant relationship between financial risk-taking and password generation, whereas Egelman and Peer (2015) did not. We suggested the use of a risk scale that is appropriate for security domain. Our results from H1 provide consistent support for risk-security behavior relationship across all SeBIS domains (device securement, password generation, proactive awareness and updating). Our study is the first to find support for risk – 'device securement' relationship compared to previous SeBIS studies.

Based on these results, we propose the use of security-context risk as appropriate in SeBIS studies. Future research could also test the proposed changes to SeBIS dimensions. Specifically, we suggest that the item 'I use a PIN or passcode to unlock my mobile phone (Device Securement)' needs modification due to the advances in biometric authentication methods available on mobile phones. Further, we suggest that "When browsing websites, I mouse over links to see where they go, before clicking them (Proactive awareness)" be modified. This present study and previous research has found that this item cross-loads on different dimensions of SeBIS.

No differences in device securement were found for age, gender, education and experience. In addition to Gratian et al. (2018)'s lack of support for this SeBIS dimension indicates further examination is needed. Results suggest that females generated weaker password generation behaviors than males. In addition, youngest group in our sample had weaker password generation behaviors. This pattern of results is similar to Sheng et al. (2010)'s study where young, female respondents are susceptible to phishing.

Significant differences for awareness dimension were found for age, education and experience. Respondents, who are older, have higher education and experience have better security awareness. These results provide indirect support for inclusion of training programs as a way to raise awareness. Further, for updating dimension, differences were found for experience and gender. Females are risk averse (Harris et al., 2006), and it is likely that females see updating as a change and therefore unwilling to take that chance. Experienced individuals might know the potential problems of outdated software and are more willing to update. Our study is the first to find support for influence of education and experience in SeBIS studies.

CONCLUSION

Understanding behavioral security is important and therefore, the need for a tool such as SeBIS that can measure broad range of security behaviors. In this study, we further test the SeBIS scale and provide some suggestions on improving the scale. Further, we establish a consistent risk-security behavior relationship by using a security domain appropriate risk scale. Finally, our study establishes individual differences that were previously undiscovered. We believe that this study adds to literature by extending the work on SeBIS scale, and contributing to establishment of a predictive tool for security behaviors.

APPENDIX A

	1	2	3	4	5
SeBIS1ssUPD	**.821**	-.018	-.007	.081	.168
SeBIS2ssUPD	**.791**	.240	.183	.101	.082
SeBIS3ssSEC	.171	.182	.109	**.659**	.001
SeBIS4ssSEC	.088	.088	.022	**.822**	.038
SeBIS5ssSEC	.238	.071	.043	.320	**.739**
SeBIS6ssSEC	-.045	-.115	.104	**.728**	.189
SeBIS7ssPA	.225	**.623**	.119	.111	.274
SeBIS8ssPA	-.134	**.534**	.374	.263	-.247
SeBIS9ssUPD	**.673**	.184	.326	.043	-.117
SeBIS10ssPA	.374	**.387**	.084	.322	**-.404**
SeBIS11ssPA	.061	**.781**	.020	-.058	.129
SeBIS12ssPG	.231	.360	**.545**	-.030	-.041
SeBIS13ssPG	.113	.121	**.701**	.074	-.110
SeBIS14ssPG	-.136	.229	**.638**	.087	.439
SeBIS15ssPG	.266	-.050	**.746**	.157	.110
SeBIS16ssPA	.143	**.569**	.155	.060	-.165

Table A1: Five Factor solution for SeBIS

	Updating	Pwd Gen	Pro. Aware	Dev Secu
SeBIS1ssUPD	**.841**	-.013	-.032	.115
SeBIS2ssUPD	**.817**	.149	.258	.122
SeBIS9ssUPD	**.670**	.297	.198	.013
SeBIS3ssSEC	.176	.119	.185	**.649**
SeBIS4ssSEC	.106	.016	.112	**.835**
SeBIS6ssSEC	-.031	.116	-.101	**.749**
SeBIS7ssPA	.251	.157	**.572**	.149
SeBIS8ssPA	-.127	.314	**.600**	.228
SeBIS11ssPA	.067	.060	**.722**	-.051
SeBIS12ssPG	.240	**.531**	.372	-.053
SeBIS13ssPG	.123	**.664**	.171	.042
SeBIS14ssPG	-.089	**.703**	.162	.158
SeBIS15ssPG	.268	**.758**	-.048	.132
SeBIS16ssPA	.144	.065	**.672**	.016

Table A2: Four factor solution for SeBIS

REFERENCES

1. Agomuoh, F. (2017). Password-free smartphones are no longer the stuff of science fiction — they're everywhere. Retrieved from https://www.businessinsider.com/smartphone-biometrics-are-no-longer-the-stuff-of-science-fiction-2017-12
2. Aurigemma, S., and Mattson, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. Information and Computer Security, 25(4), 421-436. doi:doi:10.1108/ICS-11-2016-0089
3. Becker, M. H. (1974). The health belief model and personal health behavior. Health education monographs, 2, 324-473.
4. Berns, B. (2017). Driving User Adoption: Making Sure Your Employees Are Engaged Users. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2017/06/30/driving-user-adoption-making-sure-your-employees-are-engaged-users/#4e3e42434c1a
5. Biometrics-today. (2016). Biometric smartphones to reach 100% adoption as Samsung brings iris biometrics to market. Biometric Technology Today, 2016(9), 1. doi:https://doi.org/10.1016/S0969-4765(16)30129-1
6. Biometrics-today. (2017). Number of vendors selling biometric smartphones up by 274%. Biometric Technology Today, 2017(2), 3. doi:https://doi.org/10.1016/S0969-4765(17)30027-9
7. Blais, A.-R., and Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations.
8. Chatterjee, S., Sarker, S., and Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. Journal of Management Information Systems, 31(4), 49-87.
9. Chen, H., and Li, W. (2017). Mobile device users' privacy security assurance behavior. Information and Computer Security, 25(3), 330-344. doi:http://dx.doi.org/10.1108/ICS-04-2016-0027
10. Cram, W. A., D'arcy, J., and Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43(2), 525-554.
11. Egelman, S., Harbach, M., and Peer, E. (2016). Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS). Paper presented at the Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, California, USA.
12. Egelman, S., and Peer, E. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). Paper presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea.
13. Garbarino, E., and Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. Journal of Business Research, 57(7), 768-775. doi:https://doi.org/10.1016/S0148-2963(02)00363-6
14. Gratian, M., Bandi, S., Cukier, M., Dykstra, J., and Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. Computers and Security, 73, 345-358. doi:https://doi.org/10.1016/j.cose.2017.11.015
15. Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. Journal of Management Information Systems, 28(2), 203-236. doi:10.2753/MIS0742-1222280208
16. Haag, S., and Eckhardt, A. (2014). Sensitizing employees' corporate IS security risk perception. Paper presented at the Thirty Fifth International Conference on Information Systems, Auckland, NZ.

17. Hanoch, Y., Johnson, J. G., and Wilke, A. (2006). Domain Specificity in Experimental Measures and Participant Recruitment:An Application to Risk-Taking Behavior. Psychological Science, 17(4), 300-304. doi:10.1111/j.1467-9280.2006.01702.x
18. Harris, C. R., Jenkins, M., and Glaser, D. (2006). Gender differences in risk assessment: why do women take fewer risks than men? Judgment and decision making, 1(1), 48-63.
19. Herath, T., and Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165. doi:https://doi.org/10.1016/j.dss.2009.02.005
20. Herche, J., and Engelland, B. (1996). Reversed-Polarity Items and Scale Unidimensionality. Journal of the Academy of Marketing Science, 24(4), 366-374. doi:10.1177/0092070396244007
21. Hinton, P. R., McMurray, I., and Brownlow, C. (2004). SPSS explained: Routledge.
22. IBM. (2018). Future of Identity Study. Retrieved from https://www-03.ibm.com/press/us/en/pressrelease/53646.wss#_ftn1
23. Jaeger, L. (2018). Information security awareness: literature review and integrative framework. Paper presented at the Proceedings of the 51st Hawaii International Conference on System Sciences.
24. Johnston, A. C., and Warkentin, M. (2010). FEAR APPEALS AND INFORMATION SECURITY BEHAVIORS: AN EMPIRICAL STUDY. MIS Quarterly, 34(3), 549-A544.
25. Liang, H., and Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394-413.
26. Luarn, P., and Lin, H.-H. (2005). Toward an understanding of the behavioral intention to use mobile banking. Computers in Human Behavior, 21(6), 873-891.
27. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017). Individual differences and Information Security Awareness. Computers in Human Behavior, 69, 151-156. doi:https://doi.org/10.1016/j.chb.2016.11.065
28. Menkhoff, L., Schmidt, U., and Brozynski, T. (2006). The impact of experience on risk taking, overconfidence, and herding of fund managers: Complementary survey evidence. European Economic Review, 50(7), 1753-1766. doi:https://doi.org/10.1016/j.euroecorev.2005.08.001
29. Mitnick, K. D. (2003). Are You the Weak Link? Harvard Business Review, 81(4), 18-20.
30. Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.
31. OTA. (2018). Cyber Incident and Breach Trends Report. Retrieved from https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf
32. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers and Security, 66, 40-51. doi:https://doi.org/10.1016/j.cose.2017.01.004
33. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers and Security, 42, 165-176. doi:https://doi.org/10.1016/j.cose.2013.12.003
34. Pew Research Center. (2017). Americans and cybersecurity. Retrieved from http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
35. Raubenheimer, J. (2004). An item selection procedure to maximize scale reliability and validity. SA Journal of Industrial Psychology, 30(4), 59-64.

36. Rolison, J. J., Hanoch, Y., Wood, S., and Liu, P.-J. (2014). Risk-Taking Differences Across the Adult Life Span: A Question of Age and Domain. The Journals of Gerontology: Series B, 69(6), 870-880. doi:10.1093/geronb/gbt081
37. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA.
38. Shiau, W.-L., and Chau, P. Y. (2016). Understanding behavioral intention to use a cloud computing classroom: A multiple model comparison approach. Information and Management, 53(3), 355-365.
39. Siponen, M., and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-A412.
40. Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005). Analysis of end user security behaviors. Computers and Security, 24(2), 124-133. doi:https://doi.org/10.1016/j.cose.2004.07.001
41. Swar, B., Hameed, T., and Reychav, I. (2017). Information overload, psychological ill-being, and behavioral intention to continue online healthcare information search. Computers in Human Behavior, 70, 416-425.
42. Szrek, H., Chao, L.-W., Ramlagan, S., and Peltzer, K. (2012). Predicting (un) healthy behavior: A comparison of risk-taking propensity measures. Judgment and decision making, 7(6), 716.
43. Tamilmani, K., Rana, N. P., and Dwivedi, Y. K. (2020). Consumer acceptance and use of information technology: A meta-analytic evaluation of UTAUT2. Information Systems Frontiers, 1-19.
44. Thompson, N., McGill, T. J., and Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. Computers and Security, 70, 376-391. doi:https://doi.org/10.1016/j.cose.2017.07.003
45. Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., and Bailey, M. (2016). Users really do plug in USB drives they find. Paper presented at the Security and Privacy (SP), 2016 IEEE Symposium on.
46. Trang, S., and Brendel, B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. Information Systems Frontiers, 21(6), 1265-1284.
47. Vance, A., Brinton Anderson, B., Brock Kirwan, C., and Eargle, D. (2014). Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG). Journal of the Association for Information Systems, 15(10).
48. Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425-478. doi:10.2307/30036540
49. Wash, R., Rader, E., and Fennell, C. (2017). Can People Self-Report Security Accurately?: Agreement Between Self-Report and Behavioral Measures. Paper presented at the Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, Colorado, USA.
50. Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799-2816.
51. Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., and Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Computers in Human Behavior, 84, 375-382. doi:https://doi.org/10.1016/j.chb.2018.02.019