McNair Research Journal SJSU

Volume 15 *Spring 2019* Article 4

2019

Individual Differences in Cyber Security

Christopher Conetta
San Jose State University

Christopher Conetta

Major:
Psychology

Mentor:
Dr. David Schuster

Individual Differences in Cyber Security

Biography

Christopher's belief in the importance of education stems from his roots as a first-generation college student. This passion for education is what sprouted his interest in obtaining a PhD in psychological research. His research interests include: motivation, self-efficacy, personality, performance, behavior and end-users in cyber security. Understanding how things work and improving the lives of others is what drives Christopher's research. Working as a communications intern for the County of Santa Cruz Human Services Department has given Christopher professional experience in organizational development. Currently, Christopher volunteers as an undergraduate research assistant for Vectr lab which molded his research experience in the field of human factors. In addition, Christopher volunteers at a local elementary school teaching students to code. In his off time, Christopher enjoys skateboarding, photography, film, fishing, gardening, and eating new foods with the people who make them.

Individual Differences in Cyber Security

Abstract

A survey of IT professionals suggested that despite technological advancement and organizational procedures to prevent cyber-attacks, users are still the weakest link in cyber security (Crossler, 2013). This suggests it is important to discover what individual differences may cause a user to be more or less vulnerable to cyber security threats. Cyber security knowledge has been shown to lead to increased learning and proactive cyber security behavior (CSB). Self-efficacy has been shown to be a strong predictor of a user's intended behavior. Traits such as neuroticism have been shown to negatively influence cyber security knowledge and self-efficacy, which may hinder CSB. In discovering what individual traits may predict CSB, users and designers may be able to implement solutions to improve CSB. In this study, 183 undergraduate students at San José State University completed an online survey. Students completed surveys of self-efficacy in information security, and cyber security behavioral intention, as well as a personality inventory and a semantic cyber security knowledge quiz. Correlational analyses were conducted to test hypotheses related to individual traits expected to predict CSB. Results included a negative relationship between neuroticism and self-efficacy and a positive relationship between self-efficacy and CSB. Overall, the results support the conclusion that individual differences can predict self-efficacy and intention to engage in CSB. Future research is needed to investigate whether CSB is influenced by traits such as neuroticism, if CSB can be improved through video games, and which are the causal directions of these effects.

Introduction

A survey of IT professionals (Crossler, 2013) suggested that despite technological advancement and organizational procedures to prevent cyber-attacks, users are still the weakest link in cyber security. Subsequently, it is beneficial to further investigate how appropriate responses to cyber risks, called cyber security behavior (CSB), affect individual and organizational security. Despite the advancement of security technology, there has been an increase in attacks utilizing social engineering, such as phishing, which exploits a user's individual vulnerabilities in order to gain access into enterprise computers and personal devices. Hummel (2017) summarized Verizon and Symantec's yearly analysis and discovered that phishing attacks more than doubled between October 2015 and March 2016, rising from 48,114 to 123,555. Analysis of large-scale attacks, such as the Sony Pictures hack in 2014, found that the hack was successful due to a mistake made by one employee (Pelgrin, 2014). However, it is difficult to determine why the employee was vulnerable to the attack, due to the protection of personal information and their identity. This event leaves unanswered questions about how vulnerable employees can be exploited, and if individual characteristics of employees can predict this susceptibility. With this understanding, organizations could be better protected.

Today, technology is used in an endless number of daily information management and communication tasks, such as reaching out to loved ones, completing work tasks, and filing tax returns. As a result, the information we share online is sensitive, and criminals have adopted digital strategies to exploit their victims. By obtaining unauthorized information from users' computers, hackers can leverage the victims' vulnerabilities in many ways, such as identity theft (Frank & Werner, 2007). For example, ransomware has turned into a 70 million-dollar per year criminal enterprise (Everett, 2016). Therefore, it is important to determine what precautionary behavior or technology is necessary to prevent cyber-crime. Objective knowledge of the necessary precautions can be provided by cyber professionals, and other IT staff, but such knowledge is only half of the battle. If precautionary behavior or technology is necessary, it will only protect users who engage in those

behaviors. Understanding the factors that predict user engagement in proactive cybersecurity is the focus of this research.

What Should Users Do?

Reeder, Ion, & Consolvo (2017) interviewed 231 computer security experts to discover what advice they would give to typical users. For this study, Reeder et al. (2017) recruited computer experts through Google's online security blog. Experts were identified as someone who had five or more years of experience working or studying computer security. Experts' responses were then grouped into 152 pieces of advice (Reeder et al., 2017). All pieces of advice reported by more than four experts were categorized into 15 groups. From this, the top three pieces of advice were regularly updating the operating system (suggested by 90 experts), using unique passwords (suggested by 68), and using strong passwords (suggested by 58). However, Reeder et al. (2017) concluded that only giving users the top three pieces of advice is insufficient because the other less mentioned pieces of advice are equally important. This illustrates the difficult issue of simplifying computer security while communicating best practices, so that the user can successfully adopt the best practices.

As discussed earlier by Reeder et al. (2017), cyber security is complex, which requires knowledge of many disparate behaviors to effectively secure devices. Kelly (2018) distinguished between two observable categories of these behaviors: *threat response* and *cyber hygiene.* Threat response is a user's "ability to prevent an attack from occurring by responding to a specific threat, as well as being able to stop an occurring attack" (Kelly, 2018, p. 129). Some of these responses include correctly identifying phishing emails, scanning a computer for viruses after a warning, and restoring a system to eliminate a virus. Generally, threat response is a user's ability to respond to threats as they attack or attempt to attack their computers. Cyber hygiene is "proactively minimizing vulnerabilities to maintain system security" (Kelley, 2018, p. 129). Examples of this include utilizing strong and unique passwords, backing up data, regularly updating and scanning for computer viruses (Reeder et al., 2017). Overall, cyber hygiene is defense against potential

attacks and threat response is a reaction to combat current or previous attacks.

Individual Differences

Pelgrin (2014) suggested that constant vigilance is necessary in the ever-changing cyber security threat landscape. One solution to help alleviate users' potential susceptibility to cyber security threats is to develop a way to identify those who are most and least vulnerable. This information would allow a user to potentially evaluate the time and cost necessary to elevate cyber security vulnerabilities. Therefore, it is critical that a user can effectively identify potential cyber security vulnerabilities by using strong measures that will predict future performance. Specifically, Bandura (1982) argued that self-efficacy can be a strong predictor of performance behavior. It has also been suggested that effective self-efficacy measures which maximize the prediction of future performance, should be tailored to measure the domain of interest (Bandura, 1986). Therefore, in an effort to enhance someone's ability to protect themselves online, continuously tailoring and comparing specific measures to discover what unique traits make a user more or less susceptible to cyber security threats would help trainers maximize their training effectiveness (Pelgrin, 2014).

Knowledge

Knowledge is a prerequisite for a user to intentionally execute effective SCB. According to research conducted by Arachchilage and Love, (2014) as a user's level of cyber security knowledge increases, so does their CSB. It was discovered that users high in phishing threat avoidance knowledge led to increased phishing attempt avoidance behaviors and a lack of knowledge was associated with decreased phishing attempt avoidance behavior (Arachchilage & Love, 2014). In addition, knowledge of cyber threat consequences lead to increased caution and awareness behaviors when users were online (Ben-Asher & Gonzalez, 2015). Unfortunately, knowledge of proactive CSB is not sufficient. Liang and Xue (2010) concluded that to increase a user's CSB, they need to understand cyber security threats exist and that those threats can be

avoided. If a user can detect a threat, but they believe it cannot be avoided, they will not execute proactive CSB to avoid it.

Self-Efficacy

Bandura (1982) suggests self-efficacy can be a strong predictor of performance behavior. "When beset with difficulties, people who entertain serious doubts about their capabilities slacken their efforts or give up altogether, whereas those who have a strong sense of efficacy exert greater effort to master the challenges" (Bandura, 1982, p. 123). Generally, Bandura (1986, 1997) proposed that self-efficacy influences: (1) situations and activities which affect choice behavior, (2) the extent of effort and persistence that individuals will exert to overcome adverse circumstances, (3) the feeling of stress and anxiety, and (4) performance and coping behavior. Consequently, self-efficacy may influence an individual's willingness and ability to comply with training in proactive CSB.

Knowledge affects self-efficacy. Hasan (2003) stated that prior experience with programming and computer graphics applications was shown to increase a user's computer self-efficacy beliefs. This supports claims by Bandura (1986) that self-efficacy is significantly influenced by prior experience, specifically with difficult and unfamiliar tasks (Hasan, 2003). These studies indicate that prior experience and the acquisition of knowledge may be related to a user's self-efficacy.

While it may seem intuitive that knowledge leads to self-efficacy, the reverse has also been demonstrated. Research by Gist, Schwoerer, and Rosen (1989) demonstrated that self-efficacy positively influences the acquisition and application of declarative knowledge in software training contexts (Martocchio, 1997). Martocchio's (1997) study revealed self-efficacy positively correlated to learning in an introductory Windows 3.1 training course.

Self-efficacy has been shown to predict proactive CSB. Rhee, Kim, and Ryu (2009), found that individuals with higher self-efficacy in information security use more security protection software and that individuals with higher self-efficacy in information security demonstrate more security conscious care behavior. They also found that self-efficacy in information security predicted the adoption of cyber security applications, tools, and the applying of updates. Most importantly, high

self-efficacy in information security scores predicted usage of security software and security care behavior related to computer/internet usage such as backing up important information more frequently, and the use of multiple strong passwords.

Thatcher & Perrewé's (2002) findings suggest stable traits may positively influence computer self-efficacy. Willingness to try new informational technology was positively correlated with computer self-efficacy (Thatcher & Perrewé, 2002). Compeau (1995) found that users with "high self-efficacy used computers more, derived more enjoyment and experienced less computer anxiety" (p. 203).

Personality

Traits such as neuroticism have been shown to negatively influence cyber security knowledge and self-efficacy, which may hinder proactive CSB (Halevi et al., 2016; Kelley, 2018; Semsek, 2011). Kelley's (2018) study found that neuroticism negatively correlated with semantic knowledge. Costa and MacCrae (1992) discovered that individuals who were high in neuroticism tended to also be anxious.

The previously mentioned studies support the idea that neurotic users may push cyber security alerts to the side or give up all together in an effort to reduce their anxiety. This seems like a plausible explanation, as Halevi et al. (2016) found neuroticism to be inversely related to self-efficacy. Similarly, Semsek (2011) found a negative correlation between computer anxiety and computer self-efficacy. It was also discovered that those who were low on self-efficacy also tended to dwell on personal deficiencies (Bandura, 1991) causing the individual to become more self-diagnostic than task diagnostic (Kanfer, 1987). Self-diagnosis is associated with less effective learning (Martocchio, 1997).

In another study, it was suggested that traits such as neuroticism should be broken down and studied specifically (Thatcher & Perrewé, 2002). For example, trait anxiety (TA) had a positive association with computer anxiety (CA). High negative affect users had a negative experience regardless of the situation while high trait anxiety users experienced anxiety under specific situations using information technology (Thatcher & Perrewé, 2002). In turn, this information may assist IT specialists in designing training programs to effectively increase

a user's computer self-efficacy (Thatcher & Perrewé, 2002). These findings support the notion that cyber-design could be more effective if it was able to consider the users personality when designing and operating defense technology, as personality traits were found to be a significant factor in predicting user behavior across different cultures (Helveti et al., 2016). Other findings indicate that individual traits such as neuroticism might be related to self-efficacy, which may also influence CSB.

Multiple studies have shown that lower levels of self-efficacy correlate with increased levels of anxiety in users which may impede their ability to effectively identify and execute correct CSB as technology continues to grow (Halevi et al., 2016; Liang & Xue, 2010; Semsek, 2011; Thatcher & Perrewé, 2002). A possible explanation for this is Bandura's (1986, 1997) theory which states that self-efficacy reduces a user's anxiety levels. In addition, Bandura (1982) and Brockner (1979a, 1979b) have suggested that end users with high self-efficacy tend to show lower levels of anxiety and increased positive affect, retain more, and better focus on tasks.

Statement of Purpose and Hypotheses

In discovering if self-efficacy is related to vulnerabilities of users, this information can inform trainers and help provide a more effective training program. Considering the ever-evolving threat landscape, it is beneficial to continuously measure and update scales as technology changes in order to accurately assess the threat landscape. This would also allow users to assess their own vulnerabilities in an effort to enhance their CSB. Improved training programs will reduce the potential of cyber security threats, as well as save time and money for users and organizations globally. However, there are few current cyber security training products that use a measurement to effectively identify strong and vulnerable users by focusing on individual differences. Lack of knowledge of how personality predicts CSB may be limiting the usefulness of personality measurement in cybersecurity training. By discovering what individual differences influence cyber security behavior, we can better identify who needs training and improve the content of training.

The goal of this study was to investigate the factors that predict how vulnerable users are to cyber security threats. The factors investigated

include knowledge, self-efficacy, and personality. The research reviewed here has suggested that neuroticism may affect users' self-efficacy in information security and CSB, leading to the following hypotheses:

Hypothesis 1. Neuroticism is inversely related to self-efficacy.

Hypothesis 2. Neuroticism is inversely related to CSB.

Consistent with previously mentioned studies, I propose that users with higher self-efficacy in information security will exhibit the necessary CSB in the following hypothesis:

Hypothesis 3. Self-efficacy is positively related to threat response.

Hypothesis 4. Self-efficacy is positively related to cyber hygiene.

Hypothesis 5. Self-efficacy is positively related to CSB.

Hypothesis 6. Self-efficacy is positively related to general controllability.

I also hypothesized that knowledge level of cyber security preventative measures would increase a user's self-efficacy and SCB in the following hypotheses:

Hypothesis 7. Self-efficacy is positively related to knowledge.

Hypothesis 8. Knowledge is positively related to CSB.

Methods

Participants

Participants were San José State University Students recruited through the Sona Systems research participant system. Students enrolled in introductory psychology courses were given credit upon completion of the online survey. Sona recorded a total of 200 recruited participants, but 183 responses were collected. The resulting sample (N = 183) was comprised of 24.6% male and 72.1% female participants. Six participants left gender blank which accounted for 3.3% of the sample. The average age of participants was 19 (M = 18.5, SD = 2.84). Seven participants left the text box for age blank, one participant indicated they were three years old and one participant indicated they were nine; these were interpreted as typos. Two participants wrote "Over 18" in the text box, so age could not be determined. A total of 11 participants thus did not have ages specified, accounting for 5.9% of the sample.

Measures

Knowledge Quiz. To test for participants' knowledge of SCB, participants were presented with a 16-question quiz. The first set of nine questions of the quiz was derived from Pew Research Center's cyber security quiz (Olmstead & Smith, 2017). From these questions, one question had seven options, one question and six options, four questions had five options, three questions had three options and five question had four options. Two questions were derived from Microsoft's cyber security IQ quiz which had four options each (Microsoft, 2017).

General Controllability. Users' belief in technology's ability to keep devices secure was assessed using three questions from Rhee's (2009) general controllability survey ($\alpha = 0.697$):

1. In general, threats to information security are controllable.
2. In general, technology is advanced enough to prevent information security threats.
3. In general, there exist means to control information security threats.

Questions were answered on a 7-point Likert-type scale ranging from 1 (s*trongly disagree*) to 7 (*strongly agree*).

Intentional Cyber Security Behavior (SeBIS). To measure intent to comply with current security preventative measures, this study utilized Eagleman's Security Behavior Intention Scale (SeBIS; 2015). The survey was comprised of 16 items ($\alpha = 0.801$). Each item was measured on a 5-point Likert-type scale with the following anchors: 1 (*never*), 2 (*rarely*), 3 (*sometimes*), 4 (*often*), and 5 (*always*). The original SeBIS was divided into four sub categories, however, for this study in was divided into two following the approach of Kelley (2018). The first category is cyber-hygiene, defined as any question which asked the participant how often they engaged in proactive CSB. The second category is threat-response, defined as any question which asked the participant how they would respond to a threat. The survey assessed user's intention to engage in proactive awareness, password use, regularly updating devices, and general device securement. An example of a statement used is "I manually lock my screen when I stem away from it" (Egelman, 2015, p. 2879).

Self-Efficacy in Information Security (SEIS). To measure self-efficacy in cyber security, participants were given Rhee's Self-Efficacy in Information Security (SEIS; 2009). This survey was comprised of 11 questions ($\alpha = 0.965$) which were answered on a 7-point Likert scale ranging from 1 (s*trongly disagree*) to 7 (*strongly agree*).

Personality. Personality was measured using Gosling, Rentfrow, & Swann's (2003) Ten Item Personality Inventory (TIPI). The TIPI is a brief version of personality measures which was comprised of 10 questions to assess participants Big 5 personality traits. Participants rated a list of personality traits on a 7-point Likert-type scale ranging from 1 (s*trongly disagree*) to 7 (*strongly agree*).

Demographics Questionnaire. A 16 question demographics questionnaire was given to participants asking individuals age, gender, and average use of internet for typical activities.

Procedure

Once recruited through Sona Systems, participants were then given a link to complete the survey through Qualtrics in the following order, self-efficacy in information security, general controllability, security behavior intention scale, personality measure, knowledge quiz, and demographics questionnaire.

Results

Descriptive Statistics

From the sample of 183 participants, there were a few participants with missing data. Three participants had missing data on the general controllability measure which accounted for 1.64% of the sample. Two participants had missing data for the SEIS measure which accounted for 1.09% of the sample. A total of 13 participants had some or all missing data on the SeBIS which accounted for 7.1% of the sample. Four participants did not complete any questions on the survey and there was a total of six participants who had missing data, which accounted for 3.28% of the sample. On the knowledge quiz, 15 participants left a question blank which accounted for 8.2% of the sample. For the knowledge quiz, any unanswered question was interpreted as an incorrect answer. In order to

maximize statistical power of the sample, pairwise deletion was used on the remaining surveys.

Intercorrelations Among Individual Differences

As a check for the personality measurement, bivariate correlations among other personality traits and between demographic questions were examined. Significant correlations among personality traits were between neuroticism and agreeableness (r = -.175, N = 177, p = .020), neuroticism and extraversion (r = -.171, N = 178, p = .023), neuroticism and contentiousness (r = -.343, N = 178, p < .001), and neuroticism and openness to experience (r = -.217, N = 178, p = .004). Additional correlations were found between extraversion and agreeableness (r = -.172, N = 177, p = .022), extraversion and conscientiousness (r = .156, N = 178, p = .037), extraversion and neuroticism (r = -.171, N = 178, p = .023), and extraversion and openness to experience (r = .337, N = 178, p < .001).

From the demographics survey, there was a significant negative correlation between neuroticism and usage of internet for games (r = -.180, N = 177, p = .017) and between threat response behaviors subscale of CSB and extraversion (r = -.151, N = 175, p = .047).

Tests of Hypotheses

To test Hypothesis 1, that neuroticism would inversely correlate with self-efficacy, a correlational analysis was conducted. A correlational analysis found a negative correlation between neuroticism measured by the TIPI and self-efficacy measured by the SEIS (r = -.176, N = 176, p = .020).

To test Hypothesis 2, that neuroticism is inversely related to CSB, a correlational analysis was conducted. There was no statistically significant correlation found to support Hypothesis 2. There was no significant relationship between neuroticism and the SeBIS total score (r = - .014, N = 168, p = .857), neuroticism and the threat response behavior subscale of CSB measured by the SeBIS (r = -.147, N = 175, p = .053), neuroticism and the cyber hygiene behavior subscale of CSB measured by the SeBIS (r = .082, N = 171, p = .289).

Supporting Hypothesis 3, that self-efficacy is positively related to threat response, was a significant positive relationship between self-efficacy measured by the SEIS and threat response behavior subscale of SCB measured by the SeBIS (r = .349, N = 175, p < .001).

Supporting Hypothesis 4, that self-efficacy is positively related to cyber hygiene, was a significant relationship between self-efficacy as measured by the SEIS and the cyber hygiene behavior subscale of CSB measured by the SeBIS (r = .373, N = 172, p < .001).

Supporting Hypothesis 5, that self-efficacy is positively related to CSB, was a significant relationship between the SEIS and SeBIS total score (r = .430, N = 169, p < .001).

To test Hypothesis 6, that self-efficacy is positively related to general controllability, a correlational analysis was conducted. There was no statistically significant correlation found to support Hypothesis 6. There was no significant relationship between self-efficacy and the general controllability measure (r = .136, N =179, p = .070).

Supporting Hypothesis 7, that self-efficacy is positively related to knowledge, was a significant relationship between the SEIS and the knowledge quiz (r = .233, N =176, p = .002).

Supporting Hypothesis 8, that knowledge is related to CSB, was a significant relationship between knowledge and SeBIS total score (r = .223, N = 168, p = .004).

Table 1
Correlation Matrix

		N	M	SD	1	2	3	4	5	6	7	8	9	10	11
1	Self-efficacy in Information Security (SEIS)	180	46.22	11.64											
2	Threat Response (SeBIS)	177	15.95	3.09	.35**										
3	Cyber Hygiene (SeBIS)	173	38.67	4.56	.37**	.27**									
4	Security Behavior Intention Scale (SeBIS)	170	54.62	6.14	.43**	.70**	.88**								
5	Knowledge Quiz	178	8.22	2.77	.23**	.25**	0.15	.22**							
6	Neuroticism	178	7.56	2.67	-.18*	-0.15	0.08	-0.01	-0.14						
7	Extraversion	178	7.49	3.02	0.01	-.15*	-0.09	-0.14	-0.14	-.17*					
8	Agreeableness	177	9 . 6	1.92	-0.00	0.02	.19*	0.15	0.13	-.18*	-.17*				
9	Conscientiousness	179	10.39	2.03	0.19	0.01	0.07	0.08	0.07	-.34**	.156*	0.15			
10	Openness to Experience	179	9.82	2.18	0.04	0.08	-0.06	-0.01	-0.02	-.22**	.34**	-0.02	.19*		
11	Use of Internet for Gaming	178	2.16	7.76	-0.03	-0.06	-0.04	-0.06	0.06	-.18*	0.04	0.02	0.08	0.04	
12	General Controllability	181	13.19	8.23	0.14	0.07	0.11	0.11	-0.05	-0.03	-0.11	0.08	0.01	-0.09	-0.02

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Discussion

All but one of the hypotheses were supported. Overall, the results support the conclusion that individual differences can predict self-efficacy and intent to engage in CSB. Considering the ever-changing threat landscape in cyber security, and given previous research on neuroticism, it is unsurprising that highly neurotic users would exhibit lower levels of self-efficacy. Individuals scoring higher on neuroticism tend to be more anxious, and individuals suffering from social anxiety have been shown to avoid unpleasant situations in an attempt to lower their anxiety. Respectively, it seems plausible that neuroticism may lower a user's self-efficacy in information security; feeling unable to improve one's own security may be an outcome of anxiety.

This research also demonstrates that Bandura's (1982), theory that self-efficacy is a strong predictor of behavior holds in a cybersecurity context. Thus, it may likely explain why self-efficacy would predict CSB, as found in this research. I also hypothesized that neuroticism would inversely relate to CSB. Although neuroticism inversely correlated with self-efficacy, and self-efficacy predicted security behavior intention, no statistically significant relationship was found between neuroticism and CSB. One possible explanation is the measure for CSB (SeBIS) could not accurately assess a user's intention to comply with security preventative measures. For instance, users may have chosen acceptable answers which did not reflect their actual intended behavior, thus biasing the results. The behavior intention scale focused on current best practices which are somewhat commonly known. The SEIS is better understood, with items requiring more expertise in computers not commonly held by the average college student. Questions like this make it more difficult for a user to over or underestimate their ability. It is also possible, although not able to be demonstrated here, that self-efficacy mediates the relationship between neuroticism and CSB. Bandura (1986, 1997) proposed that self-efficacy influences the feeling of stress and anxiety, and performance and coping behavior. It is possible that a user's lack of belief in their ability to effectively comply with proactive CSB might cause an increase in their anxiety. As previously discussed, anxious individuals may avoid situations which increase their anxiety. It is likely that individuals low in cybersecurity self-efficacy might avoid cybersecurity related activities in

an effort to reduce their anxiety. In turn, this would have a negative impact on their CSB. Therefore, increasing a user's self-efficacy may cause a decrease in neuroticism and an increase in proactive CSB.

An unexpected but significant negative correlation was found between neuroticism and use of internet for gaming. The more often someone reported using the internet for gaming, the more likely they were to score low on the reported neuroticism personality trait. Although spurious correlations are possible, recently, gamers have been recognized as top candidates for cyber security careers (Elder, 2018). In McAfee's (2018) report, they suggested "Gamers quickly learn to continually look for clues, tools and weapons in their quest for success. And they develop persistence, endurance, observation, and logic" (MacAfee, 2018, p. 10). This may explain why users who are more neurotic report lower use of the internet for videos games and lower levels of SEIS. Although there was no direct correlation between CSB and gaming, this finding gives some insight into what traits or hobbies may or may not influence cyber security awareness. Also, considering current research by Elder (2018) and McAfee (2018) has demonstrated gamers are ideal candidates for cyber security careers, it would be worth investigating if CSB can be improved through video games. Video gaming may be an individual difference worth exploring in future research.

Additional positive correlations were found between agreeableness and cyber hygiene. Costa and MacCrae (1992) describe agreeableness as a trait which involves interpersonal behavior. Considering the ever-evolving cyber security threat landscape, often users reach out to their social connections in an effort to obtain the most updated and effective CSB advice. Specifically, agreeableness is associated with trust, straightforwardness and compliance (Costa & MacCrae, 1992). It seems likely that individuals high in agreeableness might reach out to their trusted social circles in an effort to enhance their compliance with beneficiary agreeable CSB. In addition, individuals high on agreeableness have been shown to experience positive affect when engaging in agreeable behavior (Moskowitz & Cote, 1995). This could mean that when individuals high in agreeableness engage in agreeable CSB, it may also cause them to experience positive affect. Therefore, this research suggests

that engaging users through their social networks may be promising for increasing cyber hygiene, if only for individuals high in agreeableness.

Limitations

Due to the survey-based study being conducted online, there was a relatively high rate of participant nonresponse. It is possible that the lack of responding or lack of attention to the responses affected participant's responses. For example, two participants reported that after opening the Qualtrics link through Sona Systems, they started the survey and paused to come back later but were unable to do so. Additional limitations include a lack of diversity amongst gender, with the majority of the sample comprised of female participants.

Conclusion

Future research would benefit from exploring these personality traits further to better understand the relationships among these constructs, such as through mediated relationships. Additionally, an investigation of neuroticism, self-efficacy in information security and cyber security behavior intention involving a diverse group of post-college students or working professionals would help increase the generalizability of the research. Considering that the finding for neuroticism and self-efficacy support previous research outside of cybersecurity, it may be beneficial to construct and validate a training which targets a user's self-efficacy.

References

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122–147. https://doi.org/10.1037/0003-066X.37.2.122.

Bandura, A. (1986). Social Foundations of Thought and Action: A Social-Cognitive View. *Academy of Management Review*, *12*(1), 169–171. https://doi.org/10.5465/AMR.1987.4306538

Bandura, A. (1991). Social cognitive theory of self-regulation. Organizational behavior and human decision processes, 50, 248-287.

Bandura, A. (1997). Self-efficacy: The exercise of control. New York, NY: Freeman.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51–61. Retrieved from http://www.sciencedirect.com/science/article/pii/S0747563215000539

Brockner, J. (1979a). Self-esteem, self-consciousness, and task performance. Journal of Personality and Social Psychology, 3 7, 447-461.

Brockner, J. (1979b). The effects of self-esteem, success-failure, and self-consciousness on task performance. Journal of Personality and Social Psychology, 37, 1732-1741.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *19*(2), 189–211. https://doi.org/10.2307/249688.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010.

Costa, P. T., & MacCrae, R. R. (1992). Revised NEO personality inventory (NEO PI-R) and NEO five-factor inventory (NEO-FFI): Professional manual. Psychological Assessment Resources, Incorporated.

Elder, J. (2018). Winning the Game at McAfee: How Gamers Become Cybersecurity Workers. Retrieved from https://securingtomorrow.mcafee.com/business/winning-the-game-at-mcafee-how-gamers-become-cybersecurity-workers/

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior ever follows intention?: A validation of the security behavior intentions scale (SeBIS). In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 5257–5261). New York, NY, USA: ACM. https://doi.org/10.1145/2858036.2858265.

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2873–2882). New York, NY, USA: ACM. https://doi.org/10.1145/2702123.2702249.

Everett, C. (2016). Ransomware: to pay or not to pay? *Computer Fraud & Security*, *2016*(4), 8–12. https://doi.org/10.1016/S1361-3723(16)30036-7

Frank, C. E., & Werner, L. A. (2007). Getting A Hook On Phishing, 11.

Gist, M. E., Schwoerer, C., & Rosen, B. (1989). Effects of alternative training methods on self-efficacy and performance in computer software training. Journal of Applied Psychology, 74, 884-891.

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the Big-Five personality domains. *Journal of Research in Personality*, *37*(6), 504–528. https://doi.org/10.1016/S0092-6566(03)00046-1

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., … Chen, J. (2016). Cultural and psychological factors in cyber-security. In *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services* (pp. 318–324). New York, NY, USA: ACM. https://doi.org/10.1145/3011141.3011165.

Hasan, B. (2003). The influence of specific computer experiences on computer self-efficacy beliefs. *Computers in Human Behavior*, *19*(4), 443–450. https://doi.org/10.1016/S0747-5632(02)00079-1.

Hummel, R. (2017). Securing against the most common vectors of cyber-attacks. *SANS Institute*, 31.

Kanfer, R. (1987). Task-specific motivation: An integrative approach to issues of measurement, mechanisms, processes, and determinants. Journal of Social and Clinical Psychology, 5, 237-264.

Kelley, D. (2018). Investigation of attitudes towards security behaviors, *14*(1), 17.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(07), 394–413. https://doi.org/10.17705/1jais.00232

McAfee (2018) Winning the game. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-winning-game.pdf

Martocchio, J. J., & Judge, T. A. (1997). Relationship between conscientiousness and learning in employee training: Mediating influences of self-deception and self-efficacy. *Journal of Applied Psychology*, *82*(5), 764–773. https://doi.org/10.1037/0021-9010.82.5.764.

Microsoft. (2017). Test Your Internet Security IQ. Retrieved from http://go.microsoft.com/?linkid=9713967

Moskowitz, D. S., & Cote, S. (1995). Do interpersonal traits predict affect? A comparison of three models. Journal of Personality and Social Psychology, 69, 915-924.

Olmstead, K. & A. Smith. What Americans Know About Cybersecurity. (2017). Retrieved from http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Pelgrin, W. (2014). A model for positive change: Influencing positive change in cyber security strategy, human factor, and leadership. *NATO Science for Peace and Security Series - D: Information and Communication Security*, 107–117. https://doi.org/10.3233/978-1-61499-372-8-107.

Reeder, R., Ion, I., & Consolvo, S. (2017). 152 Simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy*.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008.

Semsek, A. (2011). The relationship between computer anxiety and computer self-efficacy. *Contemporary Educational Technology,2*(3), 177-187.

Thatcher, J. B., & Perrewé, P. L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly*, *26*(4), 381–396. https://doi.org/10.2307/4132314.