Correlating Human Traits and Cyber Security Practices of Individuals in the Philippines

Philip Kwa Teow Huat, Asian Institute of Management, Philippines
Wendy Wan Yee Hui, Singapore Institute of Technology, Singapore
Jaime Kristoffer Caig, Asian Institute of Management, Philippines
Rei Nikolai Magnaye, Asian Institute of Management, Philippines
Sharon Torreverde, Asian Institute of Management, Philippines

The Asian Conference on Arts & Humanities 2025
Official Conference Proceedings

Abstract

This paper re-examines how personality influences secure computing practices. Unlike previous studies, we focus on secure computing behavior in a Southeast Asian market, offering insights into the relationship between personality and security behavior in emerging economies. Additionally, we incorporate multifactor authentication as a key component of modern secure computing practices. To conduct our study, we used a snowball sampling technique to recruit residents of the Philippines aged 18 and above to complete an online questionnaire. The survey assessed the Big Five personality traits alongside secure computing behaviors, including software updates, device security, proactive awareness, password creation, and multifactor authentication. The questionnaire was available online for 51 days, from August 14 to October 3, 2023, and yielded 620 complete responses. Data analysis was conducted using the "seminr" package in R. Confirmatory factor analysis confirmed that our survey instruments demonstrated satisfactory reliability, discriminant validity, and convergent validity. We used Partial Least Squares Structural Equation Modeling (PLS-SEM) to examine the impact of personality on secure computing practices. To assess common method bias, we applied Harman's single-factor test and the smallest positive correlation test, both of which indicated negligible bias. Our findings align with existing literature, showing that conscientiousness and agreeableness are positively associated with secure computing practices, while neuroticism is negatively correlated. These results suggest that personality continues to shape secure computing behaviors across different cultural contexts. Organizations could enhance cybersecurity by offering tailored security training and implementing streamlined procedures that accommodate diverse personality traits, ultimately improving the protection of information systems.

Keywords: personality traits, cybersecurity behavior, human factors in cybersecurity

iafor
The International Academic Forum
www.iafor.org

Introduction

Human factors play a crucial role in cybersecurity. As Oroszi (2021) highlights, people are not only potential targets of cyberattacks but also essential defenders against them. According to the 2022 Data Breach Investigations Report by Verizon, 82% of breaches involve some form of human element, including social engineering, human error, and misuse. This high percentage underscores the importance of addressing human factors in cybersecurity.

NIST SP 800-137 defines risk as the potential threat an organization faces based on the likelihood and impact of adverse events (NIST, 2011). Human risk, specifically, refers to the losses an organization may suffer due to the actions or decisions of its people. These may include actions with negative consequences or failures to act in ways that could prevent harm. Spitzner (2022) notes that approximately 80% of global breaches involve people—often through phishing and smishing attacks, misconfigured cloud accounts, or the accidental sharing of sensitive data by IT administrators. A typical response to such incidents is to add more tools or solutions. However, this approach can increase complexity, leading to confusion and overwhelming users. For example, while stringent password policies and multi-factor authentication enhance security, they can also hinder users' ability to perform their tasks efficiently.

Given the critical role of the human element in cybersecurity, two key questions arise: (1) "How do we identify and classify individuals with strong cybersecurity behavior?" and (2) "How can we measure strong or weak cybersecurity behavior?" To address the first question, some researchers have turned to personality traits, which have profound implications for how individuals perceive and respond to cybersecurity risk situations (McCormac et al., 2017; Shappie et al., 2020). To answer the second question, a wide range of computing practices is typically considered, including password management, email use, internet use, social media use, mobile device use, information handling, and incident reporting (Egelman & Peer, 2015; Parsons et al., 2017).

Various studies have established correlations between personality and cybersecurity practices. However, security best practices evolve over time, as evidenced by the recent shift in emphasis from password use to multifactor authentication (Cyber Security Agency of Singapore, 2023). In this study, we revisit the relationship between personality and cybersecurity practices, incorporating multifactor authentication given its growing importance in the field. Importantly, we provide empirical support for the role of personality in cybersecurity using data collected from the Philippines, thereby adding a Southeast Asian context to the existing literature.

In the remainder of this paper, we will review the relevant literature, describe our research methodology, analyze our data, and discuss the implications of our findings. Finally, we will summarize the paper and outline potential directions for future research.

Literature Review

The Big Five Personality Traits model encompasses extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience, as described in Table 1. The model has been extensively researched across various domains. Studies have demonstrated its predictive power in academic performance, with conscientiousness emerging as a strong indicator of success (Nießen et al., 2020). In the realm of finance, research by Meman and

Chouhan (2021) found that extraversion and openness positively influence risk-taking in investment decisions, while neuroticism is associated with risk aversion.

Table 1
Description of the Big Five Personality Traits

Trait	Description
Extraversion	An individual's tendency to be outgoing, energetic, and sociable.
Agreeableness	An individual's tendency to be tendency to be compassionate, cooperative, and friendly towards others.
Conscientiousness	An individual's tendency to be organized, responsible, and reliable.
Neuroticism	An individual's tendency to experience negative emotions, such as anxiety, depression, and vulnerability.
Openness	An individual's willingness to engage with new ideas, experiences, and unconventional values.

Source. John & Srivastava (1999)

Security education, training, and awareness (SETA) programs are often cited as the most effective way to encourage secure computing practices among employees. However, most SETA programs are found to be ineffective in changing users' behaviors due to a lack of motivation (Noonan, n.d.). A study conducted in Norway shows that motivation to participate in online security training is influenced by personality (Vestad, 2022), suggesting that personality may be an important factor to consider when designing SETA programs.

Despite the potential significance of personality in shaping an organization's cybersecurity, relatively few studies have investigated the role of personality in cybersecurity practices. Some exceptions include Halevi et al. (2013), Riquelme and Roman (2014), Shropshire et al. (2015), McCormac et al. (2017), Shappie et al. (2020), and Kennison and Chan-Tin (2020). Key findings related to personality and cybersecurity are summarized in Table 2.

Existing empirical studies generally suggest that conscientious and agreeable individuals tend to adopt more secure computing behaviors, whereas neurotic individuals are more likely to engage in risky computing behaviors. However, the effects of extraversion and openness are mixed. These results align with our understanding of personality traits and the requirements of cybersecurity best practices. For example, highly conscientious individuals are likely to exhibit compliance behaviors (Hogan et al., 1997), including adherence to cybersecurity guidelines. Agreeable individuals tend to be more cooperative when joint action is needed (Mount et al., 1998), which is often the case in information security. Individuals with high neuroticism tend to exhibit lower levels of self-control (McCrae & Löckenhoff, 2010), which may result in risky computing behaviors. Curiosity, a core facet of openness to experience (Silvia & Christensen, 2020), may motivate individuals to pay more attention to the latest developments in cybersecurity but may also cause them to explore information beyond their access rights. Extraverts are typically communicative (Eysenck & Eysenck, 1968) and may therefore report security incidents promptly and collaborate effectively with IT and security teams, but they may be more susceptible to social engineering techniques due to their tendency to disclose personal information (Wang et al., 2021).

Different cybersecurity best practices require varying levels of effort and affect individuals differently. However, most existing studies correlate personality with a summary measure of computing practices (Kennison & Chan-Tin, 2020; McCormac et al., 2017; Shappie et al., 2020) without examining specific computing practices. Some studies focus solely on a single

computing practice, such as privacy settings (Halevi et al., 2013) or the use of specific security tools (Shropshire et al., 2015). An exception is Gratian et al. (2018), which provides a detailed and comprehensive analysis of the effects of personality traits by investigating their correlations with a variety of computing practices. However, Gratian et al. (2018) was conducted more than five years ago. In recent years, there has been a shift in emphasis from the use of passwords to multifactor authentication for access control. An update to the study is required to include this commonly adopted security measure. Furthermore, many existing empirical studies are based mostly on data collected from the US, as indicated in Table 2. There is a lack of research in a Southeast Asian context. We aim to fill this gap by collecting data on personality and cybersecurity practices from the Philippines.

Table 2
Relationships Between Big Five Personality Traits and Cyber Security

Study	Description	Country
Halevi et al. (2013)	• Openness is positively associated with weak privacy settings.	U.S.A.
Riquelme and Roman (2014)	• Extraversion is correlated with reduced perception of security risks.	Switzerland
Shropshire et al. (2015)	• Conscientiousness and agreeableness moderate the relationship between behavioral intent and extent of use of a web-based security tool.	U.S.A.
McCormac et al. (2017)	• Extraversion, agreeableness, conscientiousness and openness are positively associated with information security behavior. • Neuroticism (opposite of emotional stability) was negatively associated with information security behavior.	Australia
Gratian et al. (2018)	• Extraversion is positive associated with device securement. • Conscientiousness is positively associated with password generation and updating.	Online (87% U.S. Citizen)
Shappie et al. (2020)	• Conscientiousness, agreeableness and openness are positively associated with cyber security practices. • Neuroticism positively associated with cyber security practices.	U.S.A.
Kennison and Chan-Tin (2020)	• Neuroticism is positively associated with risk cyber security behaviors.	U.S.A.

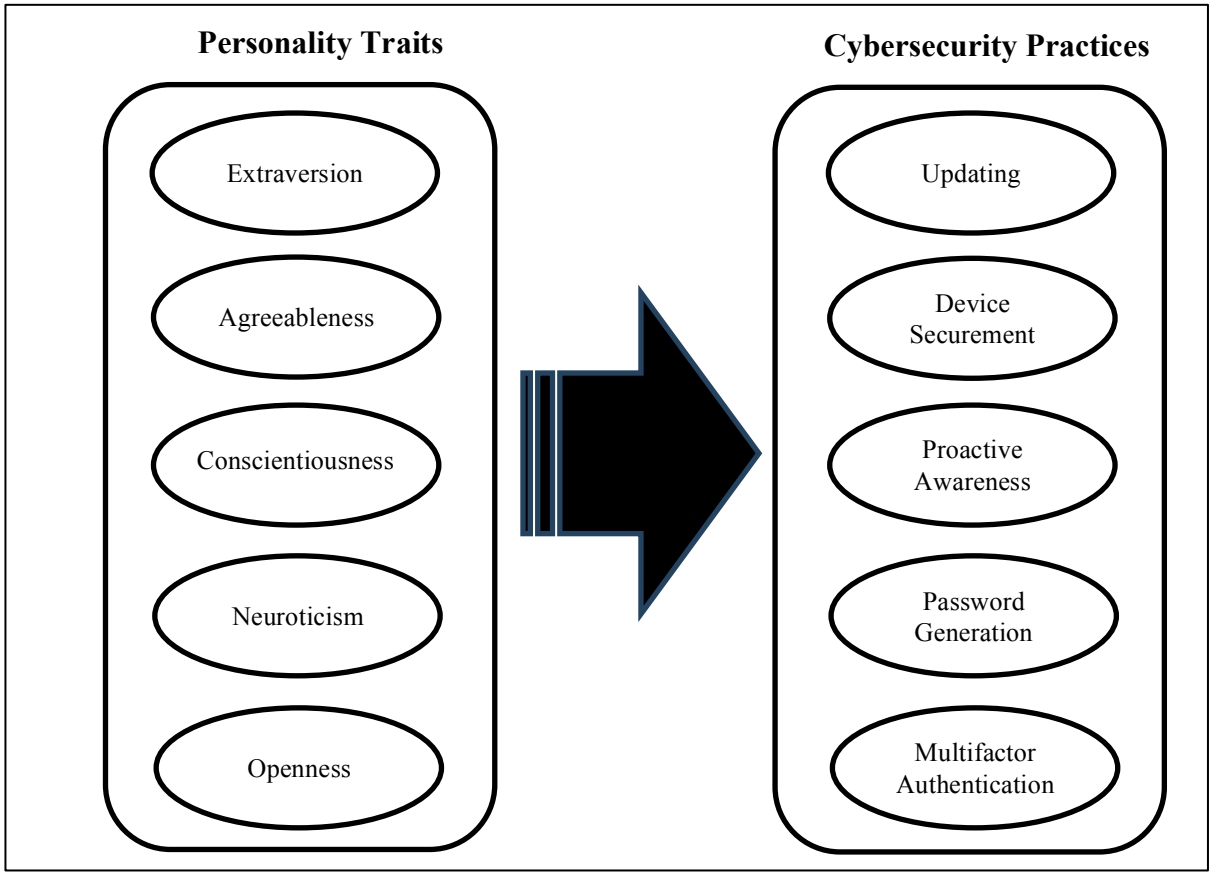
Our research model is presented in Figure 1. Specifically, we hypothesize that personality impacts cybersecurity practices. We will regress individual personality traits on each of the security practices, following Gratian et al. (2018). To avoid overwhelming the figure with too many arrows, not all hypothesized causal relationships are depicted.

Methodology

Survey Instrument

To measure personality, we use a short version of the International Personality Item Pool (IPIP) scale (Goldberg et al., 2006), which reflectively measures the five personality traits: extraversion (Ex), agreeableness (Ag), conscientiousness (Con), neuroticism (N), and openness (Op). Individuals' cybersecurity practices are measured using the Security Behavior Intentions Scale (SeBIS) developed by Egelman and Peer (2015). These practices include updating (Updating), device securement (DevSecure), proactive awareness (ProAware), and password generation (Password). We model these cybersecurity practices as constructs formatively measured by their respective indicators.

Figure 1
Research Model



In addition to the SeBIS practices, we include the use of multifactor authentication (MFA) in our survey instrument because MFA has become an essential component of Zero Trust security architecture and can significantly reduce access threats (Okta, 2021). We developed a scale that formatively measures MFA using the following items:

- "I use two-factor authentication for social media applications."
- "I use two-step verification for my email accounts."
- "I make sure that I am prompted via email or SMS when there is a login for my social media accounts from a new device."

The complete list of question items for measuring the constructs can be found in the Appendix.

Data Collection

To maximize potential survey participation across various demographics, snowball sampling was used to collect data from the researchers' contacts in the Philippines from August to October 2023. Additionally, we conducted an onsite MFA discussion in Victorias City, Negros Occidental, Philippines, and administered the online survey to 115 participants from Victorias City. All respondents were encouraged to invite their family and friends to participate in the survey. Our data collection efforts resulted in a diverse sample totaling 620 respondents, as shown in Table 1.

Data were collected using a Google Form. Only individuals with valid email addresses were able to access the survey link; however, email addresses were neither included in the data analysis nor retained for archiving. The survey link was sent to over 1,000 individuals. Respondents were required to provide consent before proceeding to the survey questions. The link remained active for 51 days, from August 14 to October 3, 2023, resulting in 620 complete responses.

Analysis

We regressed the Big Five personality traits onto each cybersecurity practice to evaluate the research model presented in Figure 1. The "seminr" package in R was used to assess both the measurement and structural models. The R script used to generate our results is available upon request.

Demographic Characteristics

We summarize some demographic characteristics of our participants in Table 3. The majority of respondents were young working adults under 35 years old. Thirty-six percent of the respondents were male, and 64% were female. Typical sectors represented by the respondents include education, information and communications technology, government, finance and insurance, healthcare, and professional business services.

Measurement Model

A confirmatory factor analysis was performed, and items that did not load well on their corresponding constructs were dropped. The reliability of our survey instrument was then assessed by examining the composite reliability and Cronbach's alpha of each reflective construct. As shown in Table 4, each construct had a composite reliability greater than 0.7, a common threshold indicating satisfactory reliability (Nunnally, 1967). Although the Cronbach's alphas are below 0.7, we administered a short version of the Big Five personality test; with fewer items, lower Cronbach's alpha values are expected. Overall, our results indicate that the instrument possesses appropriate reliability.

The numbered columns in Table 4 represent the correlation matrix between the Big Five personality constructs, with the diagonal showing the square root of each construct's AVE values. All AVE values exceed 0.5, suggesting satisfactory convergent validity. Furthermore, the square root of the AVE for each construct is greater than the correlations between that

construct and any other constructs in the model, indicating satisfactory discriminant validity (Fornell & Larcker, 1981).

In Table 5, we list the cross-loadings of the question items for the reflective constructs. All items included in our analysis load substantially higher on their corresponding factors than on other factors, providing further support for discriminant validity (Gefen et al., 2000).

Table 3
Demographic Characteristics of Survey Respondents

	Description	Count	Percentage
Gender	Male	226	36.45%
	Female	391	63.06%
	Decline to respond	3	0.48%
Age	18 - 24 years old	156	25.16%
	25 -34 years old	201	32.42%
	35 - 44 years old	142	22.90%
	45 - 54 years old	71	11.45%
	55 - 64 years old	48	7.74%
	65+ years old	2	0.32%
Education	Elementary school graduate	3	0.48%
	High school graduate	78	12.58%
	College graduate	330	53.23%
	Graduate degree or professional program completed	168	27.10%
	Other	41	6.61%
Employment Status	Student	104	16.77%
	Employed	426	68.71%
	Self-employed	39	6.29%
	Unemployed/ Unable to work/ Out of Work	33	5.32%
	Other	13	2.10%
	Retired	5	0.81%
Industry	Education	172	27.74%
	Information and Communications Technology	82	13.23%
	Government	51	8.23%
	Finance and Insurance	34	5.48%
	Healthcare	34	5.48%
	Professional and Business Services	33	5.32%
	Manufacturing	24	3.87%
	Retail and Wholesale	23	3.71%
	Transportation	6	0.97%
	Energy	4	0.65%
	Media	2	0.32%
	N/A	67	10.81%
	Other	88	14.19%

Table 4
Construct Reliability, Discriminant Validity, and Convergent Validity

	Composite Reliability	Cronbach's Alpha	1	2	3	4	5
1. Extraversion	0.838	0.625	**0.850**				
2. Agreeableness	0.878	0.728	0.152	**0.885**			
3. Conscientiousness	0.801	0.506	-0.035	0.005	**0.817**		
4. Neuroticism	0.882	0.733	0.032	0.011	-0.364	**0.889**	
5. Openness	0.795	0.504	0.040	0.047	0.298	-0.225	**0.814**

Table 5
Cross Loadings

	Extraversion	Agreeableness	Conscientiousness	Neuroticism	Openness
Ex-1	**0.793**	0.082	-0.044	0.015	0.035
Ex-2	**0.903**	0.164	-0.02	0.037	0.034
Ag-1	0.152	**0.919**	0.026	-0.013	0.052
Ag-2	0.113	**0.85**	-0.024	0.04	0.028
Con-1	-0.093	-0.078	**0.787**	-0.237	0.254
Con-2	0.026	0.075	**0.847**	-0.351	0.236
N-1	0.064	0.055	-0.358	**0.885**	-0.215
N-2	-0.005	-0.034	-0.29	**0.892**	-0.185
Op-1	0.058	0.041	0.169	-0.101	**0.732**
Op-2	0.017	0.038	0.298	-0.242	**0.888**

Path Analysis

Following the recommendation of Hair et al. (2021), bootstrapping with 10,000 subsamples was used to estimate the standard errors and evaluate the significance of the path coefficients. The path analysis results are shown in Table 6, with significant paths highlighted.

Table 6
Summary of Path Coefficients and Statistical Significance

Big Five (Antecedents)	Cyber Security Practices (Consequents)	Path Coefficient	*p*-value
Extraversion	Updating	0.049	0.2294
	Device Securement	0.029	0.4758
	Proactive Awareness	-0.121***	0.0029
	Password Generation	-0.000	0.9984
	Multifactor Authentication	-0.001	0.9769
Agreeableness	Updating	0.118**	0.0068
	Device Securement	0.161**	0.0023
	Proactive Awareness	0.028	0.4952
	Password Generation	0.014	0.7535
	Multifactor Authentication	0.117*	0.0250
Conscientiousness	Updating	0.063	0.2037
	Device Securement	0.087	0.0766
	Proactive Awareness	0.007	0.8910
	Password Generation	0.101*	0.0251
	Multifactor Authentication	0.011	0.8305
Neuroticism	Updating	0.033	0.4959
	Device Securement	-0.009	0.8438
	Proactive Awareness	-0.206***	0.0000
	Password Generation	-0.097*	0.0351
	Multifactor Authentication	0.012	0.7764
Openness	Updating	-0.004	0.9291
	Device Securement	0.057	0.1912
	Proactive Awareness	0.145**	0.0011
	Password Generation	0.081	0.0682
	Multifactor Authentication	0.072	0.1116

Evaluation of Common Method Bias

We used two different methods to assess the magnitude of common method bias. First, we performed Harman's single-factor test (Podsakoff & Organ, 1986), which uses exploratory factor analysis to determine whether all items load on a single factor; if so, common method bias is present. Our analysis showed that the total variance explained by one factor is 12.3%, suggesting that common method bias is not a serious concern. Second, to further test for potential common method bias, we used the smallest positive correlation among items as a conservative estimate (Lindell & Whitney, 2001). In our data, items Ex-2 and N-2 had the smallest positive correlation, equal to 0.000654. Following Lindell and Whitney's (2001) recommendation, we performed Fisher's r-to-z transformation on this correlation as follows:

$$z_r = \frac{1}{2}\ln\frac{1+r}{1-r} = \frac{1}{2}\ln\frac{1+0.000654}{1-0.000654} = 0.000654 \quad (1)$$

and then computed the 95% confidence interval as:

$$z_r \pm \frac{z_{1-\frac{\alpha}{2}}}{\sqrt{N-3}} = 0.000654 \pm 1.96/\sqrt{620-3} = 0.000654 \pm 0.0789 \quad (2)$$

Common method bias thus is not significant statistically, because the confidence interval includes 0.

Discussion

As expected, conscientiousness and agreeableness were found to be positively related to secure practices, whereas neuroticism showed an opposite correlation. Specifically, conscientious individuals were more likely to demonstrate better password hygiene (p = 0.0251). Agreeable individuals tended to be more diligent in updating (p = 0.0068), device securement (p = 0.0023), and multifactor authentication (p = 0.0250). Neurotic individuals tended to demonstrate lower proactive awareness (p < 0.0001) and poorer password hygiene (p = 0.0351). As expected, individuals high in openness showed a high level of proactive awareness (p = 0.0011). However, extraverts exhibited the opposite tendency (p = 0.0029).

Overall, our results show that personality continues to influence individuals' computing practices today. This finding has important HR and operational implications. Firstly, personalized training may be necessary (Rashid, n.d.). For example, training could be tailored for neurotic and extraverted individuals to improve their awareness of security threats. Wang et al. (2021) suggest that different personality traits make individuals susceptible to different social engineering exploits. For instance, individuals high in extraversion may be prone to self-disclosure; those with high conscientiousness may be vulnerable to informational influence and social responsibility norms; agreeable individuals may be susceptible to group influence and reciprocity norms; individuals scoring high in openness may fall prey to emotion-arousing techniques; and those high in neuroticism may be vulnerable to fear-arousing techniques and deindividuation. Personalized training materials could help employees defend against the social engineering attacks to which they are most vulnerable. Secondly, organizations should assign jobs requiring the handling of sensitive and critical information to individuals who are high in conscientiousness and agreeableness, as these individuals tend to exhibit organizational citizenship behavior and contribute beyond what is required by their job (Mahdiuon et al., 2010).

Finally, an organization typically consists of employees with diverse personalities. Secure computing practices should not cause excessive inconvenience or require too much effort from employees. For example, maintaining good password hygiene is often quite demanding for users (Stobert & Biddle, 2018) and can be challenging for certain personality types. A recent emphasis on the use of multifactor authentication reduces reliance on passwords, ensuring that employees who are less diligent in managing their passwords do not pose a significant risk to the organization.

Conclusion

This paper revisits the effects of personality on secure computing practices. We conducted a survey of 620 individuals in the Philippines to measure their Big Five personality traits alongside secure computing behaviors, including updating, device securement, proactive awareness, password generation, and multifactor authentication. Consistent with the literature, we found that conscientiousness and agreeableness tend to correlate positively with secure computing practices, whereas neuroticism is negatively correlated. Our results suggest that personalized security training and simplified cybersecurity processes may help organizations better safeguard their information systems.

In future research, to further highlight the significance of personality in cybersecurity, researchers may distinguish between compulsory and voluntary cybersecurity practices. Additionally, data from other regions should be collected to provide a more global perspective to the existing literature.

Declaration of Generative AI and AI-Assisted Technologies in the Writing Process

ChatGPT (GPT-4o model) was used to review the grammar of this paper.

References

Cyber Security Agency of Singapore. (2023). Importance of using secure multi-factor authentication methods. https://www.csa.gov.sg/alerts-advisories/Advisories/2023/ad-2023-006

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

Eysenck, H. J., & Eysenck, S. B. G. (1968). *Manual for the Eysenck Personality Inventory*. Educational and Industrial Testing Service.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*, *18*(3), 382–388.

Gefen, D., Straub, D. W., & Boudreau, M. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the AIS*, 4, Article 7.

Goldberg, L. R., Johnson, J. A., Eber, H. W., Hogan, R., Ashton, M. C., & Cloninger, C. R. (2006). The international personality item pool and the future of public-domain personality measures. *Journal of Research in Personality*, 40, 84–96.

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

Hair, J. F., Jr., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R*. Springer.

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd International Conference on World Wide Web* (pp. 737–744).

Hogan, R., Johnson, J., & Briggs, S. (1997). *Handbook of personality psychology* (p. 856). Academic Press.

John, O. P., & Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research* (2nd ed., pp. 102–138). Guilford Press.

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. https://doi.org/10.3389/fpsyg.2020.546546

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *83*(1), 114–121.

Mahdiuon, R., Ghahramani, M., & Sharif, A. R. (2010). Explanation of organizational citizenship behavior with personality. *Procedia - Social and Behavioral Sciences*, *5*, 178–184.

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.

McCrae, R. R., & Löckenhoff, C. E. (2010). Self-regulation and the Five-Factor Model of personality traits. In R. H. Hoyle (Ed.), *Handbook of personality and self-regulation* (pp. 145–168). Wiley-Blackwell.

Meman, M. U., & Chouhan, P. M. (2021). Big Five Personality Traits and Investment Decision. *Turkish Online Journal of Qualitative Inquiry*, *12*(9), August 2021: 896-905.

Mount, M. K., Barrick, M. R., & Stewart, G. L. (1998). The Five Factor Model of personality and performance in jobs that involve interpersonal interaction. *Human Performance*, *11*(2–3), 145–165.

Nießen, D., Danner, D., Spengler, M., & Lechner, C. M. (2020). Big Five Personality Traits Predict Successful Transitions From School to Vocational Education and Training: A Large-Scale Study. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.01827

NIST. (2011). Information security continuous monitoring for federal information systems and organizations. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

Noonan, L. (n.d.). 5 reasons security awareness training is not getting results. MetaCompliance. https://www.metacompliance.com/blog/cyber-security-awareness/5-reasons-security-awareness-training-not-results

Nunnally, J. C. (1967). *Psychometric theory*. McGraw-Hill.

Okta. (2021). Getting started with zero trust access management: Trust begins with secure identity. https://www.okta.com/sg/resources/whitepaper/zero-trust-with-okta-modern-approach-to-secure-access/

Oroszi, E. D. (2021). Exploitable traits as vulnerabilities: The human element in security. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/exploitable-traits-as-vulnerabilities

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40–51.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, *12*(4), 531–544.

Rashid, S. (n.d.). 3 ways to add personality to your security awareness programme. *MetaCompliance*. https://www.metacompliance.com/blog/cyber-security-awareness/adding-personality-to-cyber-security

Riquelme, I., & Roman, S. (2014). Is the influence of privacy and security on online trust the same for all types of consumers? *Electronic Markets*, 135–149.

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, *9*(4), 475–480.

Shropshire, S., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191.

Silvia, P. J., & Christensen, A. P. (2020). Looking up at the curious personality: Individual differences in curiosity and openness to experience. *Current Opinion in Behavioral Sciences*, *35*, 1–6.

Spitzner, L. (2022). Security awareness: It's actually about managing human risk. https://www.techuk.org/resource/sans-institute-cyber2022.html

Stobert, E., & Biddle, R. (2018). The password life cycle. *ACM Transactions on Privacy and Security*, *21*(3), Article 13. https://doi.org/10.1145/3183341

Verizon. (2022). Data breach investigations report 2022. https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

Vestad, A. (2022). Personality traits and security motivation. *Studies in Health Technology and Informatics*, *299*, 183–188.

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, *9*, 11895–11910.

Contact email: pkwa@aim.edu

Appendix: Question Items Used in the Analysis

Reflective Constructs

Extraversion	Ex-1	I am the life of the party.
	Ex-2	I talk to a lot of different people at parties.
Agreeableness	Ag-1	I sympathize with others' feelings.
	Ag-2	I feel others' emotions.
Conscientiousness	Con-1	I often forget to put things back in their proper place. (Reversed)
	Con-2	I make a mess of things. (Reversed)
Neuroticism	N-1	I have frequent mood swings.
	N-2	I get upset easily.
Openness	Op-1	I am not interested in abstract ideas. (Reversed)
	Op-2	I have difficulty understanding abstract ideas. (Reversed)

Formative Constructs

Updating	Updating-1	When I am prompted about a software update, I install it immediately.
	Updating-2	I make sure that the programs or software I use are up to date.
	Updating-3	I make sure that my anti-virus or anti-malware softwares have been regularly updating themselves.
Device Securement	DevSecure-1	I manually lock my device (laptop/desktop) screen whenever I walk away from it.
	DevSecure-2	I set my device (laptop/desktop) screen to automatically lock if I don't use it for a prolonged period of time.
	DevSecure-3	I use a PIN or a passcode or pattern to unlock my mobile phone.
	DevSecure-4	I use a password or a passcode to unlock my device (laptop/desktop).
Proactive Awareness	ProAware-1	When someone sends me a link, I immediately open it without verifying where it goes.
	ProAware-2	Whenever I encounter a security problem, I continue what I was doing because I assume someone else will fix it.
	ProAware-3	I know what website I am visiting based on its look and feel, rather than by looking at the URL bar.
	ProAware-4	When browsing website, I mouse over links to see where they go, before clicking it.
	ProAware-5	I submit information to websites without first verifying that it will be sent securely (e.g., https://, a lock icon, SSL)
Password Generation	Password-1	I don't change my passwords, unless I am prompted to.
	Password-2	I use different passwords for different accounts that I have.
	Password-3	I do not include special characters in my password if it's not required.
	Password-4	When I create a new online account, I try to create a strong password beyond the site's minimum requirements.
Multifactor Authentication	MFA-1	I use two-factor authentication for social media applications.
	MFA-2	I use two-step verification for my email accounts.
	MFA-3	I make sure that I am prompted via email or SMS when there is a login for my social media accounts from a new device.