Personality Facets and Behavior: Security Decisions under Competing Priorities

Early stage paper/Completed paper

Sanjay Goel
University at Albany, SUNY
goel@albany.edu

Jingyi Huang
University at Albany, SUNY
goel@albany.edu

Alan R. Dennis
Indiana University
ardennis@indiana.edu

Kevin **Williams**
University at Albany, SUNY
kwilliams@albany.edu

ABSTRACT

Half of all security breaches can be traced to employees not following security procedures even though they do not intend to cause harm. We theorize that this problem is not a lack of security knowledge nor willful disobedience, but rather employees making poor security decisions when trying to balance the competing priorities of their primary responsibilities against the productivity impediments that security compliance creates. We investigated the effects of security knowledge and seven personality facets from the Five Factor Model to see if there were predictable patterns in the way employees with different personalities made security decisions when faced with competing priorities. Security knowledge had no effect, suggesting that we cannot train our way out of security problems. However, six of the personality factors together had a medium effect on security decision making in situations where security compliance competes with other responsibilities. Higher dutifulness, cautiousness, achievement striving, and self-consciousness led to higher quality security decisions; higher morality led to lower quality decisions; assertiveness had mixed effects; and modesty had no effect.

Keywords

Information security, priority, security knowledge, information security awareness, dutifulness, cautiousness, achievement striving, self-consciousness, assertiveness,

INTRODUCTION

Several studies have concluded that employee behavior is the largest single root cause of security breaches, and most often it is not deliberate malfeasance that causes breaches but rather a failure to comply with security policies without malicious intent (Ernst & Young 2017; PWC 2022). A recent meta-anlysis shows that individual differences are the strongest predictor of security compliance, have a greater influence than organizational factors, such as deterance policies (Cram et al. 2019). One of the most important individual differences is personality (Costa and McCrae 1992; McCrae and Costa 1987).

Employees must make trade-offs between security compliance and their primary job responsibilities (Goel and Chengalur-Smith 2010; Posey et al. 2011), and often make deliberate decisions to place the needs of their primary responsibilities ahead of security compliance. These decisions are strongly shaped by individual differences (Cram et al. 2019), such as personality, with different employees making different trade-off decisions. Thus, it is not a lack of knowledge of security policies nor willful disobedience that leads to much non-compliance. Instead, it is dedicated employees, making considered decisions to violate security policies in order to better meet the needs of their primary responsibilities. It is not deviant or reckless employees who fail to comply, but rather those who prioritize their primary responsibilities over security.

We argue that personality traits influence how employees prioritize security compliance against primary responsibilities and thus how they make security decisions. Most personality research has

used the dominant Five Factor Model (FFM) (Costa and McCrae 1992; McCrae and Costa 1987) that posits five broad personality factors (extraversion, neuroticism, conscientiousness, agreeableness, and openness to experience) that are each comprised of six facets. The five factors are a useful, but rather blunt instrument, because they are broad collections of underlying facets of personality (John and Srivastava 1999). Past security research shows that conscientiousness predicts security behavior, but the other four factors have had quite inconsistent effects (see the next section). We argue that because we lose information as we collapse nuanced measures into broader categories (John and Srivastava 1999), the five personality factors are less useful for predicting specific behaviors (John and Srivastava 1999) such as setting strong passwords or encrypting data. As a result, focusing the more nuanced lower-level subdimensions within the five factors may enable us to better understand how individual differences influence employees to make different security decisions as they balance security compliance against their primary responsibilities.

We focus on a set of seven personality traits (i.e., facets) from the FFM to gain a deeper understanding of how personality affects the security decisions. We selected facets from four of the five major factors, focusing mostly on conscientiousness, because it has had the most consistent effects on security. We were unable to theorize that facets drawn from the Openness to New Experience would influence the security trade-off; openness is broader the other factors and its elements are not as closely related to each other (Trapnell and Wiggins 1990). Our results show that these facets are useful in explaining security decisions and offer researchers a more nuanced tool for theorizing and organizations a deeper understand of why employees make the decision they do.

THEORY AND RESEARCH

This paper focuses on non-malicious behavior (behavior that implements poor security practices without intending to cause damage (Guo et al. 2011)) because it is more common than malicious behavior (Wall 2011). Much research has examined the causes of non-malicious behavior (Bulgurcu et al. 2010; D'Arcy and Herath 2011; Johnston et al. 2016; Moody et al. 2018). Antecedents to good security practices include extra-role behaviors (Hsu et al. 2015) and job satisfaction (Greene and D'Arcy 2010), whereas antecedents to poor security behavior include moral reasoning (Myyry et al. 2009) and neutralization (Siponen and Vance 2010).

We argue that a more plausible theoretical explanation is a trade-off between primary responsibilities and security compliance. Employees face numerous time demands in their jobs and have numerous responsibilities, both to their employer and in their own personal lives. Security compliance is an additional responsibility that must be balanced and prioritized among the host of responsibilities competing for the employee's time and attention (D'Arcy et al. 2014). Complying with security policies often creates an impediment to performing primary job responsibilities (Bulgurcu et al. 2010).

When impediments from security compliance are small, the choice between security compliance and primary responsibilities is usually simple: comply and suffer the reduced productivity for the primary responsibilities. However, as the demands from primary responsibilities become stronger, the choice becomes more difficult, especially when security compliance will have a noticeable impediment on the primary responsibilities. Therefore, we hypothesize:

H1a: Situations with a higher impetus to fulfill primary responsibilities will lead to worse security decisions (compared to those with a weaker impetus).

Under this theoretical argument, security compliance is a balancing act. Employees make this decision weighing their primary job and personal responsibilities against security compliance. The choice is a personal one, influenced by the individual's knowledge and personality. Some individuals may perceive their own responsibilities to be more important than the corporate welfare promoted by security compliance; others may see breaking security rules to have a heavier cost than the impediment imposed by compliance. Therefore, we hypothesize:

H1b: The effect of personality on security compliance will be the strongest in situations with a higher impetus to fulfill primary responsibilities (compared to those with a weaker impetus).

Personality

There are many different ways of considering personality, but the dominant model is the Five Factor Model (FFM) (Costa and McCrae 1992; McCrae and Costa 1987). The FFM concludes that personality can be modeled using five key traits: extraversion, neuroticism, conscientiousness, agreeableness, and openness (McCrae and Costa 1987). Different personality factors may be more important in some contexts and less important in others. For example, conscientiousness, agreeableness, and neuroticism are related to performance primarily in jobs that rely heavily on interpersonal interaction, while agreeableness and neuroticism are more important in teamwork contexts (Mount et al. 1998). Extraversion is beneficial in contexts that involve social interaction (Barrick and Mount 1991), and openness to experience is beneficial in contexts where adaptability is key (LePine et al. 2000).

Research has linked personality traits to security decisions. Individuals high in conscientiousness are more careful, risk-averse, and self-disciplined, and are thus more likely to be aware of and comply with ISP (Alohali et al. 2018; Gratian et al. 2018; Halevi et al. 2017; Johnston et al. 2016;

Kajzer et al. 2014; McCormac et al. 2017; Pattinson et al. 2015; Shappie et al. 2020; Shropshire and Gowan 2017; Shropshire et al. 2015; van der Schyff and Flowerd 2021; Warkentin et al. 2012; Weems et al. 2019). However, research shows mixed results for the other four traits. Agreeableness has inconsistent effects on security compliance (Alohali et al. 2018), being linked to greater compliance (McCormac et al. 2017; Pattinson et al. 2015; Shappie et al. 2020) and having no effect (Gratian et al. 2018; Jaeger and Eckhardt 2021; Shropshire and Gowan 2017; Weems et al. 2019). Individuals high in extraversion are less likely (Johnston et al. 2016; Kajzer et al. 2014) or more likely (Gratian et al. 2018; Welk et al. 2015) to comply with ISP. Individuals high in neuroticism are more likely to comply with ISP (Johnston et al. 2016; Kajzer et al. 2014; McCormac et al. 2017) but are more susceptible to phishing (Halevi et al. 2013; Welk et al. 2015). Individuals high in openness make better security decisions (Shappie et al. 2020) or be less likely to comply with an ISP (Johnston et al. 2016; Kajzer et al. 2014).

Although the FFM model is useful, its five factors are intended to be very generalized groupings of related traits (Chamorro-Premuzic and Furnham 2003; McCrae and Costa 1987). Each of the five factors is in turn comprised of six distinct subdimensions, meaning that personality research suggests there are 30 distinct facets of personality (Costa and McCrae 1992). The primary advantage of the FFM model is its parsimony; only five factors. Conversely, one common complaint about the FFM is that the five dimensions are too few to accurately capture the variation in human personality (John and Srivastava 1999). Each of the five dimensions are so broad that they lose their fidelity, which is true in any hierarchical structure; we always lose information as we move up the hierarchy (John and Srivastava 1999). If we want to improve our ability to explain and predict behavior, then we may need to move down the hierarchy and use a lower level of analysis that provides more information than these five overarching factors.

In this study, we focus on individual facets that comprise these five major factors to take a more nuanced look at the effects of personality. The five major factors are summations of their underlying facets, so a look at selected facets that comprise them are likely to provide a more accurate model by enabling the researcher to select only the facets most likely to influence behavior and omitting those less likely to influence behavior (Chamorro-Premuzic and Furnham 2003). We consider the Big Five factors and the facets that comprise them below.

Conscientiousness

Conscientiousness is individual's desire to do a task well and to take obligations seriously and is manifested in the tendency for achievement striving and dependability (Barrick et al. 2001). Conscientious employees have greater attention to detail and do not accept substandard work (Shropshire and Gowan 2017). They are dependable rule-followers. Consciousness is comprised of six factors: self-efficacy, orderliness, dutifulness, cautiousness, achievement striving, and self-discipline. We selected three facets that we theorized were most related to information security behavior.

The first is dutifulness, the propensity to follow the rules, to keep promises, to do what is asked, and to tell the truth. It is the rule-following aspect of conscientiousness, so when faced with a security decision, employees with high dutifulness are more likely to place a high value on following the rules – that is, complying with organizational security policies. The second is cautiousness, the propensity to avoid mistakes, and choose carefully; it is the opposite of rashness, impulsivity, and the propensity to act without thinking. Both dutifulness and cautiousness are related to self-control (the ability to refrain from committing deviant acts), which has been linked to better security behaviors (Hu et al. 2015). Thus, we theorize that they are more likely to comply with security policies.

To these two core facets, we add a third: achievement striving, which is the propensity to work hard, accomplish goals, do more than is expected, and not do just enough to get by. We argued above that complying with security policies often creates impediments to accomplishing an employee's primary job responsibilities. Since the metrics of employees are typically bound to productivity and problem-solving, when they face with impediments, achievement striving employees are more likely to attempt to accept the impediment and take the extra time or effort to perform good security behaviors. This leads to three hypotheses:

H2a: Greater dutifulness will lead to better security decisions

H2b: Greater cautiousness will lead to better security decisions

H2c: Greater achievement striving will lead to better security decisions

Agreeableness

Agreeableness is friendly compliance, willing submission to the social group, trustfulness, and prosocial behaviors (Barrick et al. 2001; Graziano and Eisenberg 1997). Agreeableness is comprised of six facets: morality, trust, altruism, sympathy, cooperation, and modesty. We selected two facets we theorized were most related to information security behavior. The first is modesty, which is the extent to which one does not want to be the center of attention versus one who thinks highly of oneself. Individuals who score low on modesty believe they are better than others, have a high opinion of themselves, and are likely to boast about their virtue. We theorize that individuals who lack modesty will place a greater value on their own work responsibilities than on the need to comply with security policies. Thus, they will be less likely to comply when compliance creates impediments to their own work.

The second is morality, which is doing the right thing. It is rooted in the virtues and integrity of an individual and deals with conforming to standards of behavior and character based on those principles. The nature of moral reasoning that individuals use in making security decisions is nuanced and exists at different stages depending upon their moral development (Kohlberg 1984; Myyry et al. 2009). At the lowest level, moral decisions are based on avoiding sanctions for poor behavior (stage 1) or receiving compensation for good behavior (stage 2). At the next level, behavior is driven by social norms, either the norms of one's social group (stage 3) or internalized social norms (stage 4). At the highest level, behavior is driven by selecting the action that creates the greatest good for society (stage 5) or the greatest good as seen from a universal perspective (i.e., a similar act by anyone else would also be the best decision) (stage 6).

Thus individuals at the lowest levels of moral reasoning would be likely to simply comply with security policies, those in the mid-level would be influenced by the norms of their social group, and those at the highest levels would strive to balance the value of security compliance against the value of their primary responsibilities. We theorize that people who report higher morality are more likely to invoke higher levels of moral reasoning and prioritize their primary responsibilities over compliance. Thus we hypothesize:

H3a: Greater modesty will lead to better security decisions

H3b: Greater morality will lead to worse security decisions

Extraversion

Extraversion is an individual's tendency towards sociability, assertiveness, and excitement-seeking (Barrick et al. 2001). Extraverts are more friendly, cheerful, and gregarious than introverts (Costa et al. 1991). Extraversion is comprised of six facets: friendliness, gregariousness,

cheerfulness, activity level, excitement seeking, and assertiveness. We selected only one facet, assertiveness, which is the propensity to take charge, assert control, and lead others. We theorize that individuals who exhibit greater assertiveness would be more likely to lobby for the value of their own work, compared to the value of organizational security compliance. They perceive their own work to have value and thus are more likely to prioritize it above security compliance. Thus we hypothesize:

H4: Greater assertiveness will lead to worse security decisions

Neuroticism

Neuroticism is an individual's propensity to respond with negative emotions to threat, frustration, and loss (Liu et al. 2012); it is the inverse of emotional stability (McCrae and Costa 1987). Neuroticism is comprised of six facets: anger, depression, anxiety, vulnerability, immoderation, and self-consciousness. We selected only one facet, self-consciousness, which is not wanting to draw attention to one's self, being easily embarrassed, and only feeling comfortable with friends. We theorize that individuals who exhibit greater self-consciousness would be more likely to comply with organizational security policies because they do not want to draw attention to themselves by breaking rules. They are more likely to put a greater emphasis on following rules than on performing their own work. Thus we hypothesize:

H5: Greater self-consciousness will lead to better security decisions

Openness to Experience

Openness to experience is imagination, broadmindedness, and a willingness to be unconventional (Judge et al. 2002). Individuals high on openness are often artists (McCrae and Costa 1997). It is broader in scope and looser in structure than the other FFM factors, meaning its facets are not as

closely related as the facets of the other factors (Trapnell and Wiggins 1990). Its six facets are imagination, artistic interest, emotionality, action, intellect, and liberalism. We selected no facets here because we could make no theoretical arguments as to why they would affect the decision to prioritize compliance or job productivity.

METHOD

Participants

We recruited 509 participants from Amazon Mechanical Turk. Participants had to be residents of the US with full-time jobs. Seven failed the attention check leaving a final sample of 502. The average age was 33.5 (S.D.=10.5) and 62% were male.

Task and Treatments

We conducted a randomized experiment with 10 scenarios that presented a situation requiring a security decision and asked participants how likely they would be to take various possible actions. The scenarios focused on five situations (software update, storing data on a USB, data encryption, clicking on email links, and reading non-work email) and presented 3-5 possible actions that were unique to that situation. We developed a high and low strength of competing responsibilities version of each scenario; the high competing responsibilities version presented a security situation with stronger competing work or personal responsibilities than the weaker version. Participants were randomly assigned to either the five low competing responsibilities scenarios (n = 260) or the five high competing responsibilities scenarios (n = 242), with the scenarios presented in random order. The scenarios and actions were piloted test and refined prior to use. They are available from the authors.

Measures

All measures are available from the authors. The dependent measure was the quality of security decision made by the participant. Each scenario presented a set of 3-5 actions in random order (a total of 34 possible actions across all 10 scenarios). Participants were asked to rate how likely they would be to take each of the actions on a scale from 1-7 (1 = very unlikely; 7 = very likely). The security decision quality for each scenario was calculated by multiplying the participants' likelihood of performing each action by a quality score for that action, and then taking the mean across all the actions.

The quality score for each action was determined by three security experts (one security researcher, and two corporate security managers) who independently scored each of the actions on a scale of 1-10, with 1 meaning a very poor security quality action and 10 meaning a very high quality action. Inter-rater agreement was good (ICC(3, 3)=.903). The raters then discussed the differences and reached consensus on the appropriate quality score for each action. Security quality scores were centered at 5.5.

The personality facets were measured using the standard items for each facet drawn from the International Personality Item Pool (Goldberg et al. 2006; Johnson 2014). Each facet was measured using 4 items on a 1-5 point scale. All facets were reliable (cautiousness (Cronbach α =.89), dutifulness (.70), achievement-striving (.66), modesty (.79), morality (.88), assertiveness (.72)) except for self-consciousness (.58). After removing one reverse-scored item, the resulting measure for self-consciousness was reliable (.73).

As controls, we included gender and age group (18-24, 25-29, 30-34, 35-39, 40-49, 50+). Security knowledge was assessed using 11 multiple choice questions created by information security

experts. Each participant received one point for each correct answer. We excluded participants who had a lack of security knowledge (i.e., with scores of 6 or less) because most organizational employees have a reasonable understanding of security.

Procedures

The participants first read the study information sheet and answered security knowledge items. They then received five randomly assigned security scenarios in random order, and then completed the personality items, and demographics.

RESULTS

Table 1 presents the descriptive statistics and correlations among the variables. We used a SPSS GLM repeated measures analysis with security decision quality in the five scenarios as the set of dependent variables.

Factor	Mean	Std	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Encrypt Decision	10.48	4.45														
2. USB Decision	2.13	5.51	.24													
3. Update Decision	4.86	4.52	.20	-.01												
4. Email Decision	-2.44	6.45	.22	.23	.24											
5. Link Decision	-2.13	5.63	.24	.26	.13	.41										
6. Gender	0.62	0.49	-.06	.01	.03	.02	.03									
7. Competing Responsibilities	0.52	0.50	-.03	-.16	.10	.04	.04	.02								
8. Knowledge	8.17	1.07	.00	-.08	-.04	.04	.01	.00	-.04							
9. Dutifulness	3.42	1.12	-.14	-.28	-.03	-.07	-.12	-.05	-.04	.08						
10. Cautiousness	3.47	1.11	-.08	-.08	.05	.08	.01	-.09	.04	.25	.09					
11. Achievement	3.80	0.82	-.03	-.01	.06	.08	.03	-.12	-.03	.28	.15	.62				
12. Modesty	3.21	0.95	-.01	.04	.02	.08	.00	.08	-.01	.24	-.16	.42	.33			
13. Morality	3.36	1.20	-.15	-.27	-.10	-.07	-.09	-.13	-.04	.15	.80	.16	.19	.04		
14. Assertiveness	3.41	0.83	-.02	-.01	.02	-.07	.02	.03	.01	-.10	-.04	.04	.23	-.20	-.10	
15. Self-Consciousness	2.87	0.93	.03	-.05	.03	.17	.04	.00	-.03	.15	-.12	.07	-.01	.23	-.16	-.48

Table 1: Descriptive Statistics and Correlations
Note: Any correlation greater than .09 is significant at α=.05

Table 2 presents the results of the statistical analysis of the between-subjects factors influencing security decision quality, the mean beta coefficients for each factor across the five scenarios, and the effect size of every significant factor.

Factor	F	P	Effect Size (η^2)	Mean Beta
Intercept	10.034	0.002 **	0.021	20.567
Gender	0.031	0.861		0.780
Age Group	1.830	0.105		varies
Strength of Primary Responsibilities (1=stronger primary responsibilities)	10.899	0.001 ***	0.024	-10.812
Knowledge	0.592	0.442		-0.040
Knowledge x Responsibilities	0.636	0.426		0.228
Dutifulness	2.564	0.110		-0.698
Dutifulness x Responsibilities	6.914	0.009 **	0.014	0.937
Cautious	0.001	0.975		-0.793
Cautious x Responsibilities	5.132	0.024 *	0.011	1.175
Achievement	3.959	0.047 *	0.008	0.543
Achievement x Responsibilities	0.409	0.523		-0.875
Modesty	0.159	0.690		-0.689
Modesty x Responsibilities	1.078	0.300		0.974
Morality	2.136	0.145		0.117
Morality x Responsibilities	9.793	0.002 **	0.020	-1.033
Assertiveness	3.807	0.052 †	0.008	-0.815
Assertiveness x Responsibilities	5.042	0.025 *	0.011	0.884
Self-Consciousness	0.039	0.844		-0.399
Self-Consciousness x Responsibilities	6.179	0.013 *	0.013	0.666

† ≤ .10 * = p ≤.05, ** = p ≤.01, *** = p ≤.001

Table 2: Results for Security Decision Quality

The results show a significant effect for the strength of competing responsibilities: when competing responsibilities were stronger, participants made poorer quality security decisions. H1a is supported. Security knowledge was not significant. Thus, once individuals have some basic security knowledge, additional security knowledge does not lead to better decisions. This pattern of results supports our argument that it is not a lack of knowledge that leads to poor decisions, but rather the other responsibilities that compete with security compliance.

H2 examined three personality facets within the FFM's consciousness factor. The results show that achievement striving had a positive effect on security decision making for scenarios presenting both weak and strong competing responsibilities, but dutifulness and cautiousness had positive effects only for scenarios with strong competing responsibilities. Thus, H2a and H2b are partially supported and H2c is fully supported.

H3 examined two personality facets within the FFM's agreeableness factor. The results show that modesty had no significant effect on security, whereas morality had a negative effect in the scenarios with strong competing responsibilities. We note a correlation of .80 between dutifulness (rule following) and morality (not cheating), which is not surprising given their theoretical closeness. We examined the variance inflation factors (VIF) to test for multicollinearity and found all to be less than 2, except for dutifulness (3.1) and morality (3.2), which are both well below the commonly accepted level of 10 (Kutner et al. 2004); see also O'Brien (2007) who suggests that using a VIF of 10 is arbitrarily low, and argues against removing theoretically justifiable variables even in the presence of multicollinearity. We reran the model in Table 2 omitting dutifulness and the results for morality remained the same. Therefore, we conclude that these results are not due to multicollinearity; morality has a negative effect on security decisions, but modesty does not. Thus, H3b is supported, but H3a is not.

H4 examined the assertiveness personality facet within the FFM's extraversion factor. The results show that assertiveness approached significance with a negative effect on security decisions, but this was offset by an equal and opposite positive effect in the scenarios with the stronger competing responsibilities. In other words, assertiveness likely reduced compliance, but this effect disappeared under high competing responsibilities. H4 is partially supported.

H5 examined the self-consciousness personality facet within the FFM's neuroticism factor. The results show that self-consciousness had a positive effect on security decisions, but only in the scenarios with the stronger competing responsibilities. H5 is partially supported.

As we look across the pattern of results, we see that five of the seven personality factors have a significant interaction with the strength of primary responsibilities. Therefore, we conclude that H1b is partially supported: a stronger impetus to fulfill primary responsibilities sometimes makes the effects of personality stronger.

The effect sizes in Table 2 are all small, according to Cohen (1988) who defines an $\boldsymbol{\eta^2}$ effect size of .01 to be small, .06 to be medium, and .14 to be large. Of course, each personality facet does not operate independently; they are instead an integrated set of facets that work together. If we sum up the effect sizes of the significant personality facets, we see that they total .085, meaning that this set of personality facets together has between a medium and large effect size on security decision making. In other words, these six personality facets (dutifulness, cautiousness, achievement striving, morality, assertiveness, and self-consciousness) have at least a medium effect on the security decisions that employees make.

A power analysis using G*Power (Faul et al. 2007) shows that the power to detect a small effect was .96. Thus, we are reasonably confident that the factors that were non-significant do not have any effect on security decision making, at least for the 10 security scenarios we used, as understood by our participants. In other words, security knowledge and the personality facet of modesty did not play a significant or meaningful role in these security decisions.

DISCUSSION

We began by arguing that security decision-making is a balancing act in which employees must

trade-off competing responsibilities -- their primary responsibilities and complying with security policies that create impediments to performing those responsibilities. We argued that in making this trade-off, security knowledge, after reaching a certain level, would have little effect, and personality would play a stronger role. Our results show exactly that security knowledge did not influence security decisions, at least for those individuals with some basic knowledge of security. In contrast, six personality facets together had between a medium and large effect on security decision-making. Some facets had effects in situations presenting both weaker and stronger competing responsibilities to security compliance, while others had effects only in one condition or the other. Dutifulness, cautiousness, self-consciousness, and achievement striving had positive effects on security decisions, morality had negative effects, and assertiveness had mixed effects.

Implications for Theory and Research

Our results show that individuals are more likely to make poorer security decisions when faced with situations in which their primary responsibilities are stronger. Our results indicate that additional security knowledge beyond some modest baseline does not improve security decision making. We believe that when employees have a reasonable baseline of security knowledge, providing additional knowledge has little value. Instead, we view personality as an important emerging area in security research. The implication is that future theory and research should devote more attention to understanding how personality affects security decision making in a variety of different security situations and organizational contexts.

Past research has used the “Big Five” personality factors of the FFM (Costa and McCrae 1992; McCrae and Costa 1987) which are very broad (John and Srivastava 1999). In contrast, we focused our theorizing and empirical research on the lower level facets that comprise these Big Five factors. The implication is that future theory and research would benefit by redirecting some of its focus

from the Big Five factors to the lower level facets of personality. Under our theoretical framing of security decision making as a trade-off between security and work productivity, these six personality facets played important roles.

Implications for Practice

One implication for practice is that security knowledge did not matter. Once employees have some baseline security knowledge, more knowledge doesn't help. We can't educate our way out of our current information security problems; we need to look elsewhere. Our research suggests that personality should be an important focus of organizational security. Six aspects of personality had a combined effect on security decision quality that was between medium and large. People who are dutiful, cautious, achievement striving, and self-conscious tend to make better security decisions, thus they are the best to select and require less management attention. In contrast, people who are assertive tend to make worse security decisions when faced with *weaker* competing responsibilities, but this disappears when competing responsibilities are stronger. One counter-intuitive finding was that highly moral employees (those who would not cheat) are more likely to make poor security decisions when faced with strong competing responsibilities; we theorized that these employees find it easier to rationalize away their non-compliance.

Conclusion

Security decision making can be viewed as a trade-off that requires employees to balance the needs of their primary job responsibilities against the impediments created by complying with security policy. Security knowledge does not affect this trade-off (assuming some base knowledge), but personality has at least a medium effect. We believe it is time to devote more attention to the human side of the security and how personality influences security compliance.

REFERENCES

Alohali, M., Clarke, N., Li, F., and Furnell, S. 2018. "Identifying and Predicting the Factors Affecting End-Users' Risk-Taking Behavior," *Information and Computer Security* (26:3), pp. 306-326.

Barrick, M. L., Mount, M. K., and Judge, T. A. 2001. "Personality and Performance at the Beginning of the New Millennium: What Do We Know and Where Do We Go Next?," *International Journal of Selection and Assessment* (9:1-2), pp. 9-30.

Barrick, M. R., and Mount, M. K. 1991. "The Big Five Personality Dimensions and Job Performance: A Meta‐Analysis," *Personnel psychology* (44:1), pp. 1-26.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Q.* (34:3), pp. 523-548.

Chamorro-Premuzic, T., and Furnham, A. 2003. "Personality Traits and Academic Examination Performance," *European Journal of Personality* (17), pp. 237-250.

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*, (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Costa, P. T., and McCrae, R. R. 1992. "Revised Neo Personality Inventory (Neo-Pr-I)," in *The Sage Handbook of Personality Theory and Assessment*, G.J. Boyle, G. Matthews and D.H. Saklofske (eds.). Sage, pp. 179-198.

Costa, P. T., McCrae, R. R., and Dye, D. A. 1991. "Facet Scales for Agreeableness and Conscientiousness: A Revision of the Neo Personality Inventory," *Personality and Individual Differences* (12:9), pp. 887-898.

Cram, A. W., D'Arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Polict Compliance," *MIS Quarterly* (43:2), pp. 525-554.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the Is Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643-658.

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285-318.

Ernst & Young. 2017. "Ey's 19th Global Information Security Survey 2016-17."

Faul, F., Erdfelder, E., Lang, A. G., Buchner, A., and (2007). G*Power 3: A flexible statistical power analysis program for the social, b., and bio. 2007. "G*Power 3: A Flexible Statistical Power Analysis Program for the Social, Behavioral, and Biomedical Sciences," *Behavior Research Methods* (39), pp. 175-191.

Goel, S., and Chengalur-Smith, I. N. 2010. "Metrics for Characterizing the Form of Security Policies.," *Journal of Strategic Information Systems* (19:4), pp. 281–295.

Goldberg, L. R., Johnson, J. A., Eber, H. W., Hogan, R., Ashton, M. C., Cloninger, C. R., and Gough, H. C. 2006. "The International Personality Item Pool and the Future of Public-Domain Personality Measures," *Journal of Research in Personality*:40), pp. 84-96.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., and Ginther, A. 2018. "Correlating Human Traits and Cyber Security Behavior Intentions," *Computers & Security* (73), pp. 345-358.

Graziano, W. G., and Eisenberg, N. 1997. "Chapter 30 - Agreeableness: A Dimension of Personality," in *Handbook of Personality Psychology*, R. Hogan, J.A. Johnson and S. Briggs (eds.). Academic Press, pp. 795-824.

Greene, G., and D'Arcy, J. 2010. "Assessing the Impact of Security Culture and the Employee-Organization Relationship on Is Security Compliance," *5th annual symposium on information assurance (ASIA'10)*: Citeseer.

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), pp. 203-236.

Halevi, T., Lewis, J., and Memon, N. 2013. "A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits," *Proceedings of the 22nd international conference on world wide web*, pp. 737-744.

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F., and Chen, J. 2017. "Cultural and Psychological Factors in Cyber-Security," *Journal of Mobile Multimedia* (13:1&2), pp. 43-56.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., and Lowry, P. B. 2015. "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282-300.

Hu, Q., West, R., and Smarandescu, L. 2015. "The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective," *Journal of Management Information Systems* (31:4), pp. 6-48.

Jaeger, L., and Eckhardt, A. 2021. "Eyes Wide Open: The Role of Situational Information Security Awareness for Security-Related Behaviour," *Information Systems Journal* (31), pp. 429-472.

John, O. P., and Srivastava, S. 1999. "The Big-Five Trait Taxonomy: History, Measurement, and Theoretical Perspectives.," in *Handbook of Personality: Theory and Research*, L.A. Pervin and O.P. John (eds.). New York: Guilford Press, pp. 102-138.

Johnson, J. A. 2014. "Measuring Thirty Facets of the Five Factor Model with a 120-Item Public Domain Inventory: Development of the Ipip-Neo-120," *Journal of Research in Personality*:51), pp. 78-89.

Johnston, A. C., Warkentin, M., McBride, M., and Carter, L. 2016. "Dispositional and Situational Factors: Influences on Information Security Policy Violations," *European Journal of Information Systems* (25:3), pp. 231-251.

Judge, T. A., Bono, J. E., Ilies, R., and Gerhardt, M. W. 2002. "Personality and Leadership: A Qualitative and Quantitative Review," *Journal of Applied Psychology* (87:4), pp. 765-780.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A., and Bruggen, D. V. 2014. "An Exploratory Investigation of Message-Person Congruence in Information Security Awareness Campaigns," *Computers & Security* (43), pp. 64-76.

Kohlberg, L. 1984. *The Psychology of Moral Development*. New York: Harper & Row.

Kutner, M. H., Nachtsheim, C. J., and Neter, J. 2004. *Applied Linear Regression Models*, (4th ed.). McGraw-Hill Irwin.

LePine, J. A., Colquitt, J. A., and Erez, A. 2000. "Adaptability to Changing Task Contexts: Effects of General Cognitive Ability, Conscientiousness, and Openness to Experience," *Personnel Psychology* (53:3), pp. 563-593.

Liu, Y., Wang, Z. H., and Li, Z. G. 2012. "Affective Mediators of the Influence of Neuroticism and Resilience on Life Satisfaction," *Personality and Individual Differences* (52:7), pp. 833-838.

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), pp. 151-156.

McCrae, R. R., and Costa , P. T. 1987. "Validation of the Five-Factor Model of Personality across Instruments and Observers," *Journal of Personality and Social Psychology* (52), pp. 81–90.

McCrae, R. R., and Costa, P. T. 1997. "Conceptions and Correlates of Openness to Experience," in *Handbook of Personality Psychology*, R. Hogan, J.A. Johnson and S. Briggs (eds.). San Diego: Academic Press.

Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1), pp. 285-311.

Mount, M. K., Barrick, M. R., and Stewart, G. L. 1998. "Five-Factor Model of Personality and Performance in Jobs Involving Interpersonal Interactions," *Human performance* (11:2-3), pp. 145-165.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules&Quest; an Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

O'Brien, R. L. 2007. "A Caution Regarding Rules of Thumb for Variance Inflation Factors," *Quality & Quantity* (41), pp. 673-690.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., and Calic, D. 2015. "Factors That Influence Information Security Behavior: An Australian Web-Based Study," in *Human Aspects of Information Security, Privacy, and Trust*, T. Tryfonas and I. Askoxylakis (eds.). pp. 231-241.

Posey, C., Bennett, R. J., and Roberts, T. L. 2011. "Understanding the Mindset of the Abusive Insider: An Examination of Insiders' Causal Reasoning Following Internal Security Changes.," *Computers & Security* (30:6), pp. 486–497.

PWC. 2022. "2022 Global Digital Trust Insights." Retrieved 07/01/22, from https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/global-digital-trust-insights.html

Shappie, A. T., Dawson, C. A., and Debb, S. M. 2020. "Personality as a Predictor of Cybersecurity Behavior," *Psychology of Popular Media Culture* (9:4), pp. 475-480.

Shropshire, J., and Gowan, A. 2017. "Identifying Traits and Values of Top-Performing Information Security Personnel," *Journal of Computer Information Systems* (57:3), pp. 258-268.

Shropshire, J., Warkentin, M., and Sharma, S. 2015. "Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior," *Computers & Security* (49), pp. 177-191.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Trapnell, P. D., and Wiggins, J. S. 1990. "Extension of the Interpersonal Ajective Scales to Include the Big Five Dimensions of Personality," *Journal of Personality and Social Psychology* (59), pp. 781-790.

van der Schyff, K., and Flowerd, S. 2021. "Mediating Effects of Information Security Awareness," *Computers & Security* (106), p. 102313.

Wall, D. S. 2011. "Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders," in: *White Paper: Data Loss Prevention, Symantec, Mountain View, CA (http://download. channelpartner. de/files/578. pdf)*.

Warkentin, M., McBride, M., Carter, L., and Johnston, A. 2012. "The Role of Individual Characteristics on Insider Abuse Intentions," *AMCIS*, p. Paper 28.

Weems, C. F., Ahmed, I., Richard, G. G., Russell, J. D., and Neill, E. L. 2019. "Susceptibility and Resilience to Cyber Threat: Findings from a Scenario Decision Program to Measure Secure and Insecure Computing Behavior," *PLOS One* (13:12), p. e0207408.

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., and Mayhorn, C. B. 2015. "Will the “Phisher-Men” Reel You In? Assessing Individual Differences in a Phishing Detection Task," *International Journal of Cyber Behavior, Psychology and Learning* (5:4), pp. 1-17.