Pre-Employment Screening for Security Risk: An Exploratory Study

Joseph H. Schuessler
Tarleton State University

Dwight M. Hite
Cameron University

This study explores the relationship that one's personality, work ethic, computer self-efficacy, Internet anxiety, computer anxiety, as well as various demographic variables have with the strength of passwords users use with various sites that they frequently visit. Many organizations use various measurement tools to indicate the employability of potential hires. By identifying relevant measures as it relates to password complexity, and by extension, security posture, organizations could more quickly identify potential hires who require more or less security training. Results and implications are discussed.

INTRODUCTION

What if a human resource representative could assess a potential hire as a security risk during the initial employee screening process? Would that not serve as a practical measure as part of the hiring decision for that individual? But how would one do that? What are some of the relevant characteristics that would suggest to a human resource representative that one potential hire might be more predisposed to poor password practices over another potential hire? The goal of this paper is to assess some of the more practical measures that human resource employees could use in assessing potential hires as it relates to the security prowess of those potential employees. Many organizations routinely give preliminary tests to determine the suitability of potential hires to work within their organization. Cognitive ability tests (Schmidt & Hunter, 1981), personality tests (Hogan, Hogan, & Roberts, et al., 1996), and tests over content (Maurer & Alexander, 1992) such as programming are common, yet security is not something that is usually considered as part of this process. When it is considered, it is usually a separate process involving background checks and the like.

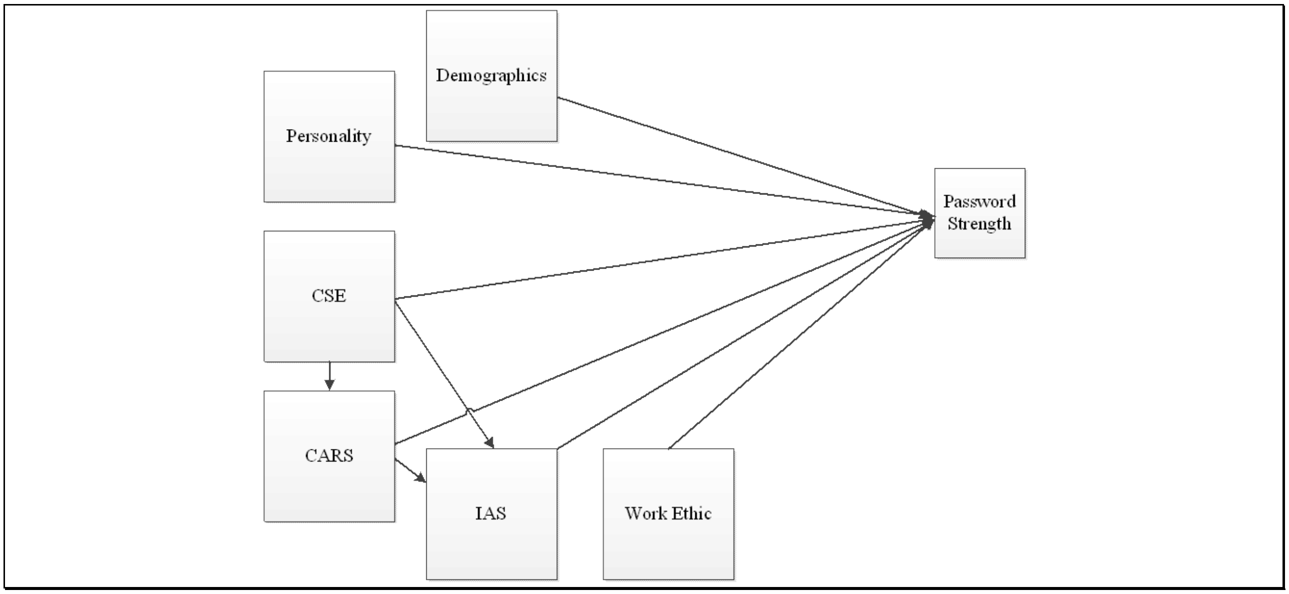
The research questions addressed by this study include: what role does one's demographic characteristics, personality, work ethic, computer self-efficacy, Internet anxiety, and computer anxiety play with respect to the strength of the passwords that they use on a routine basis? By understanding these relationships, human resource personnel can limit their pre-employment screening measurement items to only those that provide the necessary information and they can more quickly classify potential candidates with respect to their security training needs as it relates to the use of strong passwords.

LITERATURE REVIEW

Pre-Employment Screening

Davis, Flett, and Besser (2002) suggested that examining characteristics about potential hires could be used for pre-employment screening. These researchers found that by measuring problematic Internet use, one's predisposition towards procrastination, impulsivity, and social rejection could be examined. This approach suggests that during the pre-employment screening process, various other tendencies of potential hires could be qualified through testing. For example, if one could assess the work ethic of a potential hire before they were offered a position, security practices such as using strong passwords may be determined before making an offer. Similarly, one's personal characteristics could potentially lead to some insight into the password practices that a potential hire might have. The proposed research model in Figure 1 is discussed in the narrative below.

FIGURE 1
PROPOSED RESEARCH MODEL



Authentication and Passwords

Security to organizations is a primary concern for a variety of reasons (Schuessler, 2012). Countermeasures, defined as "internal and external forces that can influence whether or not a threat is able to be realized and/or affect the severity of such a threat if it were to occur" (Schuessler, 2012), are applied by organizations in an effort to protect their various assets. Of the various tenets to securing information systems is the concept of the triple-A model. AAA stands for authentication, authorization, and accounting. When implemented as part of a comprehensive security strategy, it allows an organization to authenticate its users, identify which resources each user is authorized to use, and to be able to determine the actions that each user conducted when using the organization's systems. Of the three components of the model, it is argued that the authentication step is the most important for without effective authentication, neither authorization nor accounting is able to produce results as intended.

Authentication involves accurately identifying who the potential user is. One or more of three approaches is usually used to authenticate a user's identity: what one knows, what they have, and what they are. What they are is commonly referred to as the field of biometrics. Things like facial recognition, thumb prints, hand geometry, or retina scans are all indicative of biometric devices used to authenticate a user. What you have is often referred to as a token. This may include a key fob, debit card, and so on. The final category, what you know, is usually a password or personal identification number (PIN). Of the three approaches, it is this final approach that is most commonly used (Touchette, Hewitt, & Huson, 2012). Most users are very familiar with their use, most systems have authentication systems developed around their use, and their relative costs make them a preferred choice for authenticating users.

Demographics

One's gender may be related to the strength of password(s) chosen by individuals. Often times, users are asked to provide their own passwords to access resources. Though some technical controls can be used to increase password complexity, the user's influence over the content of various passwords used is likely affected by various characteristics about a user (Touchette et al., 2012). Such characteristics, if identified, could be used to determine a user's propensity to implement and use strong passwords. Brown et al. (2004) noted that approximately two-thirds of users' passwords are based on personal characteristics. For example, their gender may indicate that a user is likely to have a more or less secure password. Brosnan and Lee (1998) and Balka and Smith (2000) suggested that males have more experience using computers. Combined with the finding by Chua, Chen, and Wong (1999) that greater levels of computer experience are associated with lower levels of computer anxiety and more positive attitudes towards computers, one might suspect that there would be differences between the genders with respect to password complexity.

Like gender, an individual's age may provide insight into whom and who may not be more likely to develop strong passwords. Results are somewhat conflicted regarding whether younger or older users use stronger passwords. Schneier (2006) found that younger users used stronger passwords when he examined the use of MySpace passwords. However, Bonneau (2012) examined Yahoo passwords and determined that older users used more complex passwords. While the former study had certain methodical constraints that limit one's ability to interpret the findings, the conflict between the two studies suggests that further study is warranted.

Yet another potential demographic variable that might be related to the strength of password chosen by users is the field in which they work. As a surrogate, this study uses the respondent's college major to identify their field (Touchette et al., 2012). Some fields such as Information Systems are more likely to instill in their students the importance and caveats in using passwords. Conversely, other fields such as Management focus more on the social aspects of business and thus, it is likely that less stress would be placed on such issues.

These hypotheses address the first research question which revolves around the various demographic variables and their relationship to the strength of the passwords that they develop.

Hypothesis 1: There is a relationship between demographic characteristics and the strength of passwords.

H_{1a}: There is a relationship between gender and password strength.

H_{1b}: There is a relationship between age and password strength.

H_{1c}: There is a relationship between major and password strength.

Personality

While demographic characteristics about users may be related to the strength of passwords chosen by users, there are likely other characteristics about users that tend to associate with the use of strong passwords as well. Personality is one such characteristic argued to influence one's strength in password choices. Shropshire, Warkentin, Johnston, and Schmidt (2006) argued that personality was positively related to the ability of users to secure their information systems within organizations. Using the Five Factor Model, they focused on two dimensions and examined their ability to predict "IT security compliant behavior." Those two dimensions were conscientiousness and agreeableness. The remaining dimensions, extroversion, neuroticism, and openness were not examined. Due to the exploratory nature of this paper, we examined each dimension as it related to the strength of passwords chosen by users.

Following in the footsteps of Shropshire et al. (2006), conscientiousness and agreeableness were hypothesized to be positively related to the strength of passwords chosen by users. Similarly, it is argued that the more neurotic an individual is, the more likely they will be to utilize strong passwords. This leads us to the following hypotheses:

> *Hypothesis 2: There is a relationship between personality and the strength of passwords.*
>
> *H_{2a}: There is a positive relationship between conscientiousness and password strength.*
> *H_{2b}: There is a positive relationship between agreeableness and password strength.*
> *H_{2c}: There is a relationship between extroversion and password strength.*
> *H_{2d}: There is a positive relationship between neuroticism and password strength.*
> *H_{2e}: There is a relationship between openness and password strength.*

Computer Self Efficacy

Computer self-efficacy (CSE) may also be related to one's ability to develop secure passwords. CSE is the degree of confidence one has in using a computer. Because CSE is an important factor in users acquiring new computing skills (Miura, 1987), those with higher CSE are likely to embrace and use technology in a variety of settings and for a variety of purposes. This additional exposure to various applications of technology may make them aware of the security concerns of such use and as a result, stronger passwords may be selected. This would be consistent with the finding by Rhee et al. (2009) in which they found that those with higher CSE resulted in stronger security behavior from those individuals with lower CSE. This leads us to our third hypothesis:

> *Hypothesis 3: There is a positive relationship between CSE and password strength.*

Computer Anxiety

Computer anxiety is defined as the fear of using or fear of potentially using computers (Chua, Chen, and Wong, 1999). The Computer Anxiety Rating Scale (CARS), a validated instrument, can be used to assess one's anxiety as it relates to computers or the potential use of computers. Because the fear of using computers can be viewed almost as the opposite of high CSE, there should be a negative relationship between CSE and CARS. This relationship is consistent with the finding by Compeau and Higgins (1995) in which they found a negative relationship between these two constructs. While this relationship is not of material importance to this study, it does help one to surmise that if the relationship between CSE and CARS is negative, the proposed relationship between CSE and strength of passwords is positive, then it is likely that the relationship between CARS and the strength of passwords is negative. This leads to the following hypothesis:

> *Hypothesis 4: There is a negative relationship between computer anxiety and password strength.*

Internet Anxiety

Similar to computer anxiety, Internet anxiety is the fear of, instead of the computer, the Internet. The Internet Anxiety Scale (IAS), another validated instrument, can be used to make this assessment. Gackenbach (1998) noted that most studies that examine computer usage and Internet usage tended to reach similar results. This suggests that since computer anxiety (CARS) should be negatively related to password strength, that Internet anxiety should, by extension, be negatively related to password strength. It also suggests that there should be a positive relationship between computer and Internet anxiety. This leads to hypothesis 5:

> *Hypothesis 5: There is a negative relationship between Internet anxiety and password strength.*

Work Ethic

The final construct examined in the current study is work ethic. One would expect that those with a stronger work ethic would be more security minded and as a result, tend to use more secure passwords. As conceptualized by Miller, Woehr, and Hudspeth (2001), the work ethic construct is multi-dimensional and consists of seven dimensions: Self-Reliance, Morality/Ethics, Leisure, Hard Work, Centrality of Work, Wasted Time, and Delay of Gratification. Self-Reliance refers to, “striving for independence in one’s daily work”; Morality/Ethics refers to, “believing in a just and moral existence”; Leisure refers to, “pro-leisure attitudes and beliefs in the importance of non-work activities” (reverse coded); Hard Work refers to, “belief in the virtues of hard work”; Centrality of Work refers to “belief in work for work’s sake and the importance of work”; Wasted Time refers to, “attitudes and beliefs reflecting active and productive use of time”; and Delay of Gratification refers to, “orientation toward the future; the postponement of rewards” (Miller, Woehr, & Hudspeth, 2001; p. 14). Each of these individuals dimensions combine to create the holistic construct of work ethic.

It has been suggested that declines in work ethic are associated with, among other things, increases in counterproductive behaviors (Sheehy, 1990). In other words, higher work ethic is associated with less risky behavior. Again, because of the exploratory nature to the current study, each dimension of work ethic is hypothesized to be positively associated with password strength, consistent with what is suggested by the overall relationship between work ethic and risky behavior.

Hypothesis 6: There is a positive relationship between work ethic and password strength.

H_{6a}: There is a positive relationship between self-reliance and password strength.

H_{6b}: There is a positive relationship between morality/ethics and password strength.

H_{6c}: There is a positive relationship between leisure and password strength.

H_{6d}: There is a positive relationship between hard work and password strength.

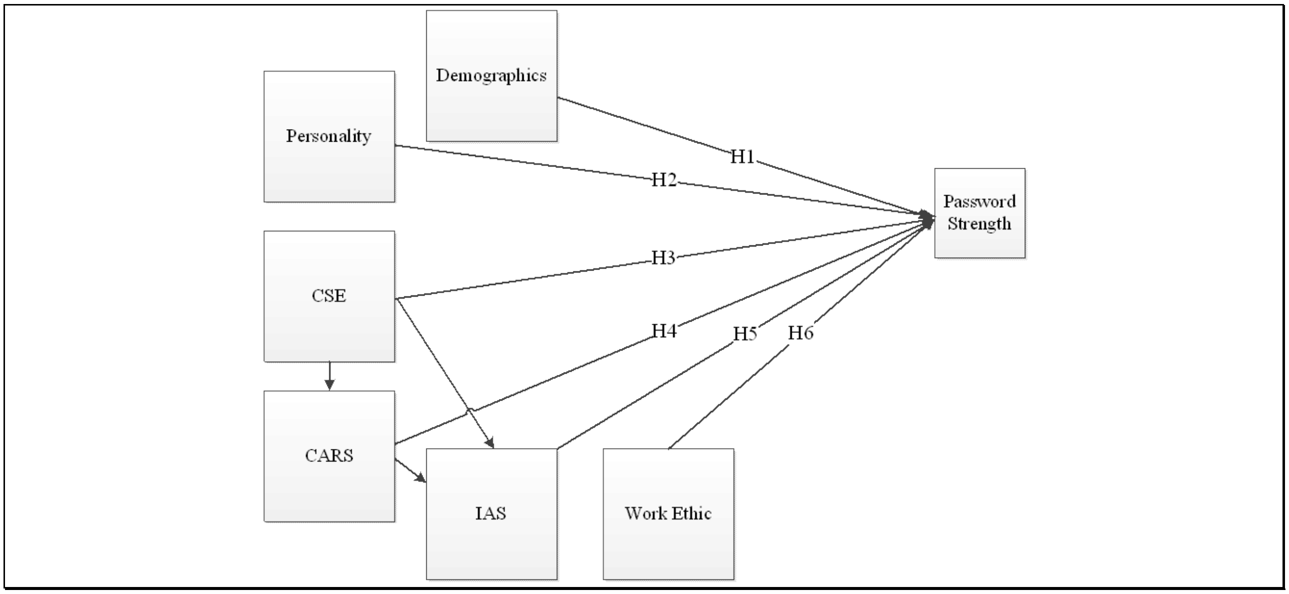
H_{6e}: There is a positive relationship between centrality of work and password strength.

H_{6f}: There is a positive relationship between wasted time and password strength.

H_{6g}: There is a positive relationship between delay of gratification and password strength.

This leads to the research model in Figure 2 below. Though the relationships between computer self-efficacy and computer anxiety and between computer anxiety and Internet anxiety are not hypothesized, they are incorporated into the model for completeness.

FIGURE 2
RESEARCH MODEL



METHODOLOGY

The study sample consisted of 122 undergraduate and graduate business students from two south central universities within the United States. Of these, 71 participants responded resulting in a 58% response rate. The participants ranged in age from 20 to 62 and the mean age was 32.7 years. 47.9% of the participants were male, while 52.1% were female. The majors of the participants included Management (28.2%), Finance (5.6%), Accounting (9.9%), Information Systems (26.8%), and other (29.6%).

Construct measures included previously developed and validated instruments, with the exception of the measure for the password construct. To measure password strength, a Microsoft® online password checker tool (https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx) was utilized to determine the strength of passwords that participants might frequently use (e.g. passwords for online banking, social networking, etc.). This tool assesses a password and indicates its strength as “weak,” “medium,” “strong,” or “best.” Hence, password strength was measured on a four-point scale. The other measurement instruments utilized within this study included the following scales. The Computer Self-Efficacy scale was developed and validated by Murphy, Coover, and Owen (1989). The Computer Anxiety Rating Scale was developed and validated by Heinssen, Glass, and Knight (1987). The Internet Attitude Scale was modified from the Computer Attitude Scale, developed and validated by Nickell and Pinto (1986), and utilized by Sam, Othman, and Nordin (2005). The Multidimensional Work Ethic Profile was developed and validated by Miller et al. (2001). The personality measure utilized in this study is a modified version of the big-five measure developed as part of the International Personality Item Pool (http://ipip.ori.org); this modified version was validated by Hite (2009).

All of the aforementioned scales, along with demographic items, were embedded into an online survey. Participants were provided a link to the online survey and given a week to complete it. Participants were awarded class credit for completing the survey.

RESULTS

The survey resulted in 71 out of 122 respondents responding. This represents a response rate of 58%. Students ranged in age from 20 to 62 with the average age being 32.7 years of age.

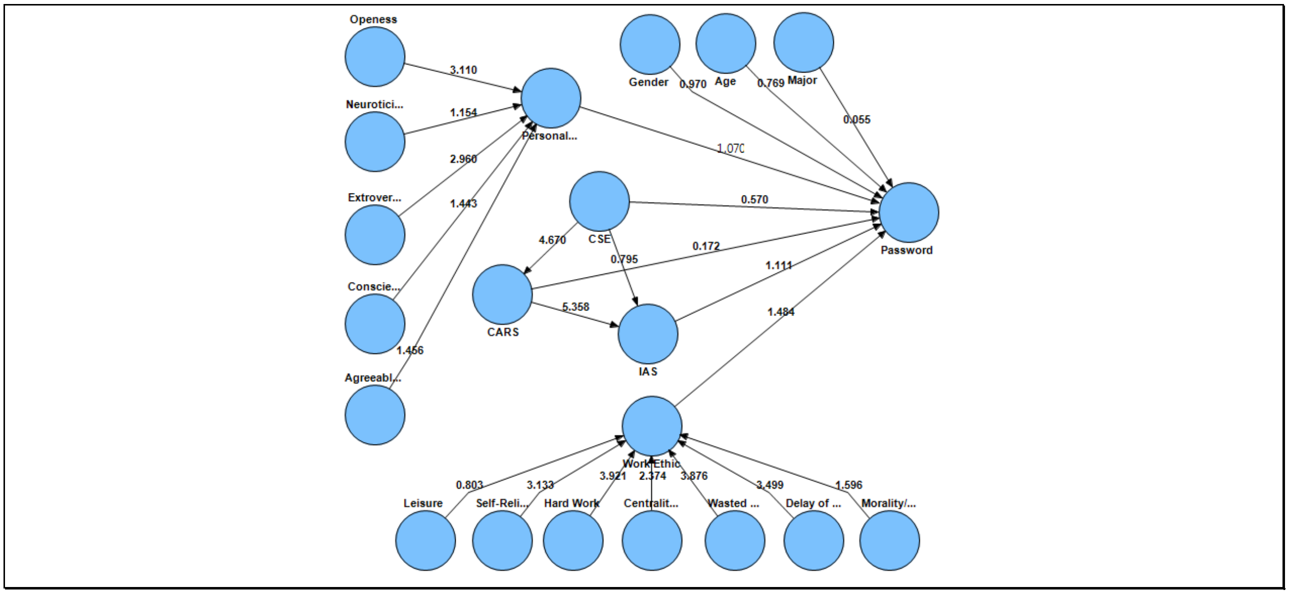
Gender was fairly well distributed with 47.9% of the respondents being male and 52.1% being female. Caucasians were the most commonly represented ethnicity in the sample representing 62% of the respondents. African Americans were the second most represented with 15.5%. The remainder of the ethnic groups was Hispanic, Native American, Pacific Islander, and other.

The majors of the respondents included Management (28.2%), Finance (5.6%), Accounting (9.9%), Information Systems (26.8%), and other (29.6%). Lastly, no freshmen responded to the survey, 4.2% were sophomores, 19.7% were juniors, 14.1% were seniors, and 62.0% were graduate students.

In all, the diversity of the makeup was fairly well distributed with the possible exception of the number of graduate students.

The initial full model was run and resulted in no significant relationships with the exception of the relationships between the dimensions of Work Ethic and the dimensions of Personality. As a result, an iterative process was conducted in order to identify a meaningful model that could be used to predict the strength of password of potential hires. Figure 3 below conveys the t-values calculated after running a bootstrap for 200 iterations.

FIGURE 3
FULL MODEL (T-VALUES)



Ultimately, it was determined that the individual dimensions of the various constructs allowed the model to predict not only significant relationships, but was also able to explain more of the variance in the strength of password use. The final model given below in Figure 4, illustrates the path coefficients and the R^2 value of the password construct. SmartPLS (Ringle, Wende, & Will, 2005) does not provide any goodness of fit indices. Rather, the significance of relationships along with the weight of each coefficient and signs are used to assess the quality of the model. Figure 4 shows that the final model was able to account for 43% of the variance in the password construct. The significance of each relationship is discussed next. The Cronbach's Alpha for each construct was generally good with only one (Conscientiousness) in the questionable range at .68. All remaining constructs were .72 or higher.

Passwords, which included online banking passwords, social network passwords, and personal email passwords, and was the only non-validated item measured, had a Chronbach's Alpha of .84.

FIGURE 4
REDUCED MODEL PATH COEFFICIENTS AND R^2 REPORTED (PLS ALGORITHM)

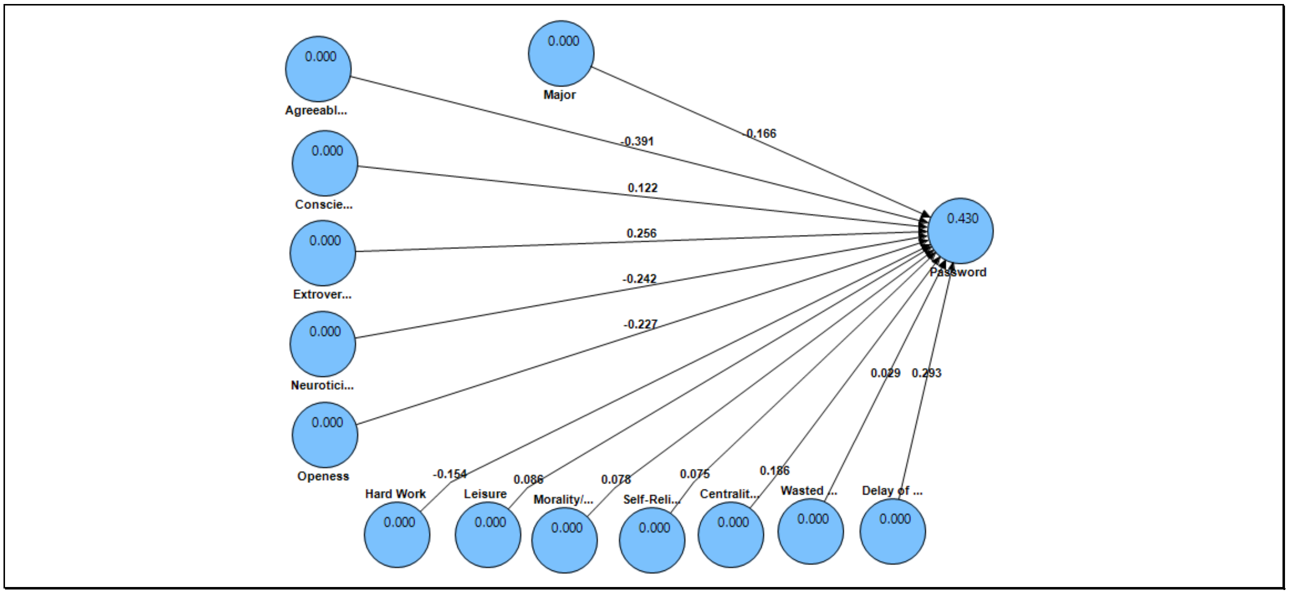


Figure 5 below illustrates the significance of each path. An alpha of .10 was chosen which is reasonable given the exploratory nature of the study. Using this as the criteria, several of the relationships were statistically significant. These are illustrated in Table 1 below. The significant relationships are bolded.

FIGURE 5
REDUCED MODEL T-VALUES (BOOTSTRAP)

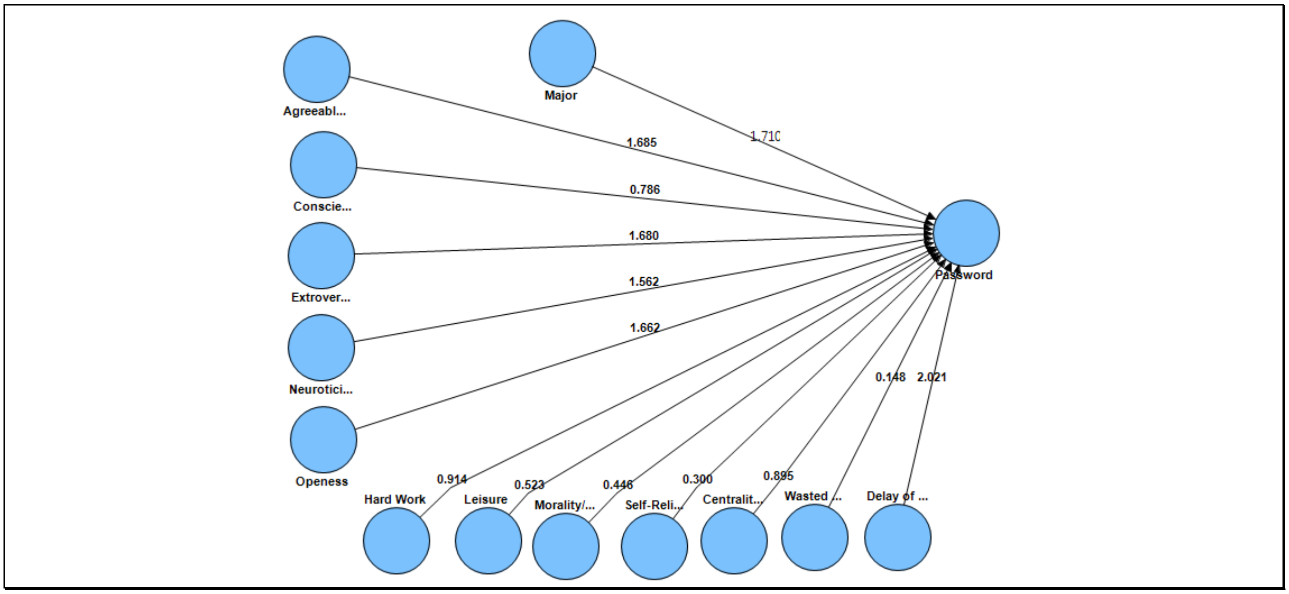


TABLE 1
HYPOTHESES RESULTS

	Original Mean	Bootstrap Mean	Standard Deviation	Standard Error	t-test	2-tailed	1-tailed
$H1_a$: Gender -> Password	*	*	*	*	*	*	*
$H1_b$: Age -> Password	*	*	*	*	*	*	*
$H1_c$: Major -> Password	**-0.166**	**-0.144**	**0.097**	**0.097**	**1.710**	**0.092**	0.046
$H2_a$: Conscientiousness -> Password	0.122	-0.016	0.155	0.155	0.786	0.435	0.217
$H2_b$: Agreeableness -> Password	***-0.391***	***-0.247***	***0.232***	***0.232***	***1.685***	*0.096*	***0.048***
$H2_c$: Extroversion -> Password	**0.256**	**0.170**	**0.153**	**0.153**	**1.680**	**0.097**	0.049
$H2_d$: Neuroticism -> Password	***-0.242***	***-0.164***	***0.155***	***0.155***	***1.562***	0.123	***0.061***
$H2_e$: Openness -> Password	-0.227	-0.169	0.137	0.137	1.662	0.101	0.050
H3: CSE -> Password	*	*	*	*	*	*	*
H4: CARS -> Password	*	*	*	*	*	*	*
H5: IAS -> Password	*	*	*	*	*	*	*
$H6_a$: Self-Reliance -> Password	0.075	-0.023	0.249	0.249	0.300	0.765	0.382
$H6_b$: Morality/Ethics -> Password	0.078	0.013	0.176	0.176	0.446	0.657	0.328
$H6_c$: Leisure -> Password	0.086	0.000	0.164	0.164	0.523	0.602	0.301
$H6_d$: Hard Work -> Password	-0.154	-0.018	0.169	0.169	0.914	0.364	0.182
$H6_e$: Centrality of Work -> Password	0.186	-0.011	0.208	0.208	0.895	0.374	0.187
$H6_f$: Wasted Time -> Password	0.029	0.062	0.195	0.195	0.148	0.883	0.442
$H6_g$: Delay of Gratification -> Password	**0.293**	**0.234**	**0.145**	**0.145**	**2.021**	0.047	**0.024**

* Results not calculated for final model since they were no longer included.
Italicized relationships were significant but in the opposite direction hypothesized.

DISCUSSION

As can be seen in Table 1 above, several of the constructs were significantly related to the strength of passwords chosen by users. Though the study was limited to College of Business students, it should come as no surprise that a relationship was found between the major of students and their propensity for selecting and using strong passwords. Used primarily as a control variable, one would expect those with a background in information systems to have a firmer understanding for the importance of strong passwords over some of the other college majors.

Agreeableness describes an individual as kind, sympathetic, and cooperative. Those who score low on this dimension tend to be more skeptical and less trustworthy of people (Graziano and Eisenberg, 1997). As a result, this “built-in” suspicion of others would suggest that such a person would be predisposed to be more proactive when it came to securing their information systems beginning with the use of strong passwords. This finding is in direct contrast with the suggestion by Shropshire et al. (2006) that agreeableness should have been positively related to security measures such as strength of passwords.

Extroversion was found to be positively related to the strength of passwords. This relationship was simply hypothesized to exist and no directionality was suggested. Further examination of this dimension of personality did not reveal any compelling reason as to why it should be related to the strength of passwords used by users. Nevertheless, this study found that there was a positive relationship found between the strength of passwords that users use and the degree of extroversion that they exhibit. Norris, Larsen, and Cacioppo (2007) and Gray (1994) suggested a negative relationship between extroversion and neuroticism. Given the neuroticism results discussed next, the relationship between extroversion and strong passwords seems to make sense but the underlying reason for this relation needs further study.

Neuroticism, like agreeableness, was significant but in the opposite direction hypothesized. Neuroticism is characterized by anxiety, moodiness, worry, envy, and jealousy (Thompson, 2008). It would seem to make sense that an individual who exhibited one or more of these characteristics might be more likely to ensure that their passwords would be "safer." However, this seemingly contrary finding can possibly be at least partially explained by the relationship between neuroticism and delayed gratification. Those who suffer from neurotic tendencies tend to have trouble with delayed gratification, suggesting a negative relationship between these two constructs. Individuals who are unable to control their need for gratification act without contemplating the implications of those actions (Krueger, Caspi, Moffitt, White, & Stouthamer-Loeber, 1994). As it relates to the current study, those who suffer from neurotic behavior generally have a need for instant gratification and as a result, tend to develop easier passwords; ones that are less likely to be forgotten, easier to recall from memory, and easier to quickly type into their system.

As hypothesized, delay of gratification was found to be positively related to password strength. While this dimension of work ethic, as the name suggests, is associated with the postponement of rewards, it is also associated with an orientation towards the future (Miller et al., 2001). Central to this dimension of work ethic is the propensity to save for the long term rather than spend in the short term, with a focus upon one's future well-being. It is likely that those who save more are also more likely to strive to protect assets in a manner such as utilizing strong banking passwords. Furthermore, those with an orientation toward the future are likely to utilize strong passwords to protect their future interests. For example, such persons may employ strong passwords on social networking sites to protect their personal and/or professional image. Altogether, individuals with heightened delay of gratification tendencies tend to utilize stronger passwords than those who lean toward instant gratification.

CONCLUSIONS

An exploratory study, this study sought to explore the relationship between personal characteristics, personality, computer self-efficacy, computer anxiety, Internet anxiety, and work ethics and the relationship each had to the strength of password chosen by users. Though computer self-efficacy, computer anxiety, and Internet anxiety could not be shown to be related to the strength of passwords, some personal characteristics, personality dimensions, and work ethic dimensions were related. These can be used by human resource personnel as an effective way of evaluating a potential hire's need for security training as it relates to passwords before making a hiring decision.

Limitations

By sampling students, it could be argued that the results do not apply to the general population. However, due to the spectrum of ages surveyed and the relatively high average age of the sample, it is argued that this sample is relatively similar to the general population, at least more so than most student samples. Another potential weakness of this study is the relatively low number of respondents. PLS is particularly well suited to use when faced with small sample sizes and was chosen for this reason (Chin, 2000).

Future Research

Future research should examine the role that personality and work ethic play in the greater security context of one's general personal security posture. Additionally, given the contrasting findings revolving around age and the strength of passwords and the lack of relationship found in this study, additional examination of this relationship is needed. Together, information gleaned from such studies could prove useful for screening potential hires before job offers are made.

REFERENCES

Balka, E. & Smith, R. (2000). *Women Work and Computerization*, Boston, Massachusetts: Kluwer.

Bonneau, J. (2012). The Science of Guessing Analyzing an Anonymized Corpus of 70 Million Passwords. *IEEE Symposium on Security and Privacy*. San Francisco, California.

Brosnan, M. & Lee, W. (1998). A Cross-Cultural Comparison of Gender Differences in Computer Attitudes and Anxiety: The UK and Hong Kong. *Computers and Human Behavior,* 14(4), pp. 559-577.

Brown, A., Bracken, E., Zoccoli, E. & Douglas, K. (2004). Generating and Remembering Passwords. *Applied Cognitive Psychology*, 18(6), pp. 641-651.

Chin, W. (2000). *Partial Least Squares for Researchers: An overview and presentation of recent advances using the PLS approach* [Power Point Slides]. Retrieved from http://disc-nt.cba.uh.edu/chin/indx.html

Chua, S., Chen, D. & Wong, A. (1999). Computer Anxiety and its Correlates: A Meta-Analysis. *Computers in Human Behavior,* 15, pp. 609-623.

Compeau, D. & Higgins, C. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly*. 19(2), pp. 189-211.

Davis, R., Flett, G. & Besser, A. (2002). Validation of a New Scale for Measuring Problematic Internet Use: Implications for Pre-Employment Screening, *CyberPsychology & Behavior,* 5(4), pp. 331-345.

Gackenbach, J. (1998). *Psychology and the Internet: Intrapersonal, interpersonal and transpersonal implications*. Academic Press, New York, New York.

Gray, J. (1994). *Personality dimensions and emotion systems. In P. Ekman & R. Davidson (Eds.), The nature of emotions: Fundamental questions* (pp. 329–331). New York, New York: Oxford University Press.

Graziano, W. & Eisenberg, N. (1997). *Agreeableness; A Dimension of Personality. In R. Hogan, S. Briggs, & J. Johnson). Handbook of Personality Psychology.* San Diego, California: Academic Press.

Heinssen, R.K., Glass, C.R. & Knight, L.A. (1987). Assessing computer anxiety: Development and validation of the computer anxiety rating scale. *Computers in Human Behavior,* 3, 49-59.

Hite, D.M. (2009). *Leader emergence and effectiveness in virtual workgroups: Dispositional and social identity perspectives*. (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI Number: 3385792).

Hogan, R., Hogan, J. & Roberts, B. (1996). Personality Measurement and Employment Decisions: Questions and Answers. *American Psychologist*. 51(5), pp. 469-477.

Krueger, R., Caspi, A., Moffitt, T., White, J. & Stouthamer-Loeber, M. (1996). Delay of Gratification, Psychopathology, and Personality: Is Low Self-Control Specific to Externalizing Problems?. *Journal of Personality*, 64(1), pp. 107-129.

Maurer, T. & Alexander, R. (2006). Methods of Improving Employment Test Critical Scores and Derived by Judging Test Content: A Review and Critique. *Personnel Psychology*. 45(4), pp. 727-762.

Miller, M., Woehr, D. & Hudspeth, N. (2001). The Meaning and Measurement of Work Ethic: Construction and Initial Validation of a Multidimensional Inventory. *Journal of Vocational Behavior*. 17(5). pp. 1-39.

Miura, I. (1987). The Relationship of Computer Self-Efficacy Expectations to Computer Interest and Course Enrollment in College. *Sex Roles,* 16, pp. 303-311.

Murphy, C.A., Coover, D. & Owen, S.V. (1989). Development and validation of the Computer Self-Efficacy Scale. *Educational and Psychological Measurement,* 49, 893-899.

Nickell, G.S. & Pinto, J.N. (1986). The computer attitude scale. *Computers in Human Behavior,* 2, 301-306.

Norris, C., Larsen, J. & Cacioppo, J. (2007). Neuroticism is Associated with Larger and More Prolonged Electrodermal Responses to Emotionally Evocative Pictures. *Psychophysiology*, 44(5), pp. 823–826.

Rhee, H., Kim, C. & Ryu, Y. (2009). Self-Efficacy in Information Security: Its Influence on End User's Information Security Practice Behavior. *Computers & Security*, 28. pp. 816-826.

Ringle, C., Wende, S. & Will, A. (2005). *SmartPLS (Version 2.0 (beta)).* Hamburg, Germany.

Sam, H.K., Othman, A.E.A. & Nordin, Z.S. (2005). Computer Self-Efficacy, Computer Anxiety, and Attitudes toward the Internet: A Study among Undergraduates in Unimas. *Educational Technology & Society*, 8(4), 205-219.

Schuessler, J. (2012). *Threats and Countermeasures of the Realm in 2011.* New Orleans, Louisiana: Proceedings of the SWDSI.

Schmidt, F. & Hunter, J. (1981). Employment Testing: Old Theories and New Research Findings. *American Psychologist*. 36(10), pp. 1128-1137.

Schneier, B. (2006). MySpace Passwords Aren't So Dumb. *Wired.com.*

Sheehy, J. (1990). New Work Ethic is Frightening. *Personnel Journal*. pp. 28-36.

Shropshire, J., Warkentin, M., Johnston, A. & Schmidt, M. (2006). Personality and IT Security: An Application of the Five-Factor Model. *Americas Conference on Information Systems (AMCIS) 2006 Proceedings*. pp. 3443-3449.

Thompson, E. (October 2008). Development and Validation of an International English Big-Five Mini-Markers. *Personality and Individual Differences*, 45(6), pp. 542-548.

Touchette, T., Hewitt, B. & Huson, M. (2012). Password Security: What Factors Influence Good Password Practices, *Proceeding of the SWDSI, New Orleans, Louisiana. 2012.*