Volume 4, No. 2
August 2011
ISSN: 1946-1836

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

In this issue:

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer-reviewed academic journal published by **EDSIG,** the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is currently semi-annual. The first date of publication is December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 45%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

JISAR Editorial Board

Password Security Risk versus Effort: An Exploratory Study on User-Perceived Risk and the Intention to Use Online Applications

Judith Gebauer
gebauerj@uncw.edu

Douglas Kline
klined@uncw.edu

Information Systems & Operations Management Department
University of North Carolina Wilmington
Wilmington, NC 28403, USA

Ling He
lhe12@svsu.edu
Department of Accounting
Saginaw Valley State University
University Center, MI 48710, USA

Abstract

We present the results of a study that explored the relationship between user-perceived security risk of online applications and the efforts associated with password use. Based on data that were collected from undergraduate students and analyzed using the Partial Least Square (PLS) method, we found that the reactions of users to efforts related with password strength differed from the reactions to efforts related with frequency of required password change. In general, long and complicated passwords appear to be more acceptable than passwords that need to be changed very often, in particular for applications that users perceive to be of high risk. The results of our study should be of interest to practitioners who need to balance organizational needs with individual user behavior when developing effective security strategies, and to researchers who are interested in the conceptualization of fit-variables.

Keywords: online applications, user-perceptions, security, risk, password strategy, fit, empirical study, PLS-analysis

1. INTRODUCTION

It is generally recognized that there are trade-offs involved with implementing information systems, such as between usability and security (DeWitt & Kuljis 2006). Common security measures attempt to increase security through dictating user behavior, such as password policies. A policy that requires, for instance, very long passwords has been shown to decrease the likelihood of the password being cracked by technical means (Lockdown 2008; Neosmart 2006; Salem, Hossain, & Kamala 2008), but it

may also be considered inconvenient, since the user must remember a lengthy string of characters that takes considerable time to type (Kuo, Romanosky, & Cranor 2006; Zhao, Wang, Wu, & Ma 2005). In addition, the policy may even be thought of as less secure to the extent that users write their passwords down and place them in close proximity to their machines, thus increasing the likelihood to be obtained by non-technical means (Gehringer 2008).

Insights about the tradeoff between usability and technical security requirements are commonly included in password policies as system administrators and business managers attempt to balance the various factors (Forget, Chiasson, Van Oorschot, & Biddle 2008; Garrison 2006). In general, it is possible to assess the consequences of inadequate password strength from an objective technical perspective, be it related to the possibility of unauthorized access to data as a result of particularly weak security, or related to performance losses and the need for additional system resources as a result of particularly strong security measures.

Less is known, though, about the differing impacts on user-behavior that result from situations of minimal versus very high levels of security, as perceived by a user (Florêncio & Herley 2007). Kline, He, & Yaylacicegi (forthcoming) found that users had an awareness of security technologies but did not always use them, and considered reputation and peer opinion more important than technological factors when judging the risk associated with a web site. Wier, Douglas, Carruthers, & Jack (2009) found that most users chose e-banking one-time passwords that were least secure, in their opinion, for convenience. Jones, Anton, & Earp (2007) found that user perceptions of authentication technologies were different in a banking setting than in a retail setting.

While users who perceive a system to exhibit an insufficient level of security may refrain from using it because of the fear of unauthorized access to sensitive information (risk), an excessive level of security may deter users because of limited usability and inconvenience (Hart 2008). System administrators are, thus, left with the challenge of developing security policies that are not only optimal from technical and organizational standpoints, but also sensitive to the consequences that the policies have for user behavior. The challenge is particularly difficult yet nonetheless critical in an open environment with a great number of users, such as a university setting. At the same time, a university setting provides the opportunity for education, whereby practical guidelines are needed to ensure effective results.

In the current study, we set out to improve our understanding of the extent to which very low levels of password security have similar or different consequences for user behavior than comparatively high levels of security. In other words, we seek to understand better the association between security as an independent variable, and a user's intention to use online information systems as the dependent variable, whereby our focus is on password policies. In particular, we address the following two research questions:

1. What is the functional relationship between password-related security requirements and the intention to use online applications?

2. What are the risk-perceptions of various types of online applications and what are the implications of user-perceived risk on user-behavior?

Our research promises insights for system and business administrators who need to provide effective information systems. The goal is to help improve security management with practices that are successful because of their comprehensiveness, as they take into consideration user preferences and behavior, in addition to the more common technical and organizational perspectives. More specifically, we hope to learn more about the practical implications of the presumed trade-off between the need for security and password-related efforts associated with the use of online applications, all from the perspective of the user. From an IS research perspective, we hope to contribute to a growing body of literature that seeks to develop a better understanding of various functional forms of fit, such as between task and technology (Gebauer 2009; Goodhue & Thompson 1995) and the respective dependent variables. The focus of the current study is on the fit between user-perceived application risk and password-related effort, and the implications for user behavior.

2. RESEARCH MODEL

The current research model (Figure 1) was developed to understand the impacts of user-perceived password-related efforts and application-related risks on the intention to use

an online application. In essence, we are interested in the interaction between the two elements of user-perceived risk (i.e., presumed need for security) and password-related effort (inconvenience). As for control factors, we use demographic aspects (age, gender, and computer knowledge) (Florêncio & Herley 2007), and type of application.

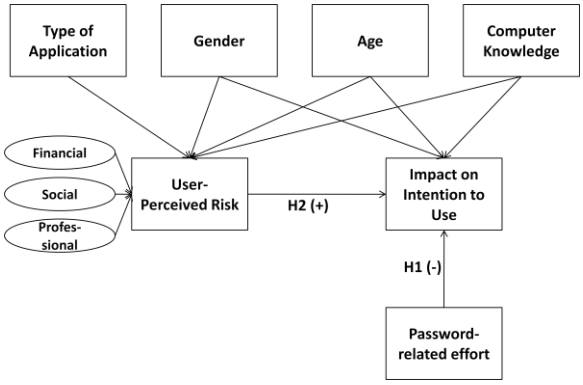

Figure 1: Research Model

Users are commonly required to enter a secret password in order to gain access to and use an online application. Password requirements are set by system administrators and vary in length, types of characters to be included, and frequency with which a password has to be changed. From the perspective of the user, password management can be seen as inconvenient because it requires extra effort, such as the effort associated with selecting a valid code and remembering or storing it. In addition, the subsequent use of a password requires a repeated extra effort before the user can access the online application. We suggest that from a user perspective, password-related efforts can be regarded as some form of costs (albeit intangible) that are associated with the use of an online application. Consequently, and all other things equal, the need to maintain and use a secret password should reduce the overall value of an online application, and may in fact deter marginal users for whom the extra efforts does not outweigh the benefit associated with using the application. We hypothesize:

H1: Password-related efforts are associated negatively with the intention to use an online application.

In other words, we expect to find that minimal required password-related efforts correspond with high values of intention to use. In contrast, higher required password-related efforts should correspond with lower values of intention to use.

However, the use of online applications comes of course with risks as a result of the open computer network structure that underlies the Internet and that can expose sensitive data to unauthorized access. Weir et al. (2007) found that context can change user perceptions of security. In the current study, we include three types of risk in the analysis: *Financial risk* relates to the negative financial implications that a user may incur when unauthorized access to account and credit card information leads to fraud or identity theft. *Social risk* relates to the negative implications that a user may incur in their personal life when information about activities or preferences is exposed to third parties without user consent. Similarly, *professional risk* relates to the negative implications that a user may incur in their professional life when sensitive information about personal preferences, activities, or health conditions are exposed to a current or future employer or school administration without user consent.

All other things equal, the risks that are associated with the use of an online application can reduce its overall value from a user's perspective, in addition to negative consequences from the perspectives of system administration and organization management. To the extent that passwords limit the risks that users associate with online applications, they can help maintain the intended benefits associated with the applications, and thus offset at least partially the hypothesized negative effects of password-related efforts. We hypothesize:

H2: User-perceived risk of an online application is associated positively with the impact of password-related efforts on intention to use an online application.

Put differently, for low levels of user-perceived risk, we expect limited or even negative effects of password-related efforts on the intention to use an online application; a user who is generally willing to comply with certain password requirements may be less inclined to do so for applications that are perceived to be of low risk. For high levels of user-perceived risk, however, we expect positive effects of password-related efforts on the intention to use an online application; a user who is generally willing to comply with certain password requirements may be even more accepting of the need for such efforts for applications that are considered to be of high risk. As the two hypothesized effects on

intention to use counteract each other, we are interested in their relative strength and interaction.

3. RESEARCH METHODOLOGY

Data Collection

Data were collected among undergraduate business students at a public university who were enrolled in an introductory course on information systems. Surveys were distributed online at two different times, January 2009 (n=200) and December 2009 (n=159). Participating students received course credit at the discretion of their respective instructor. Table 1 depicts the basic demographic data of the respondents who filled out the survey completely (n=339), including gender, age groups, and self-reported computer knowledge. For the later variable, we used a five-point Likert-scale ranging from "well below average" to "well above average". A summary of the questionnaire is provided in the Appendix.

Table 1: Demographic Data (n=339)

Variable	Value	Percentage
Gender	Male	58.1
	Female	41.9
Age	17-18	2.9
	19-20	67.4
	21-22	17.9
	23-24	5.6
	25-26	1.5
	27-30	2.1
	31-35	1.8
	35-40	0.6
	41-50	0.3
Computer Knowledge	Well below average	0.6
	Below average	4.5
	Average	55.2
	Above average	34.5
	Well above average	5.3

T-tests to assess the independence of the two data samples (January versus December) showed no significant difference for any of the three demographic variables gender ($t(339)=-0.149$, $p=0.881$), age ($t(339)=1.599$, $p=0.111$) and computer knowledge ($t(339)=0.289$, $p=0.773$). We consequently combined the data from the two surveys for the remainder of the analyses.

Measurement Scales

All model constructs were operationalized with single item indicators, except for risk, which was measured with a three-item reflective construct (Figure 1).

We coded password-related efforts with two different indicators, namely (1) required password strength pertaining to length and special characters, and (2) frequency of password change. *Password strength* was coded with a seven-level ordinal scale that included zero length/no special characters, and 4 characters, 8 characters, and 12 characters, each with and without required non-letter characters. *Frequency of password change* was coded with a four-level ordinal scale that included no required change, and required changes every year, every three months, and every week.

The main dependent variable (*intention to use*) was operationalized as the impact of password-related efforts on intention to use and measured with a five-point Likert-scale that ranged from very negative to very positive. We performed separate analyses for both types of password-related efforts (strength and frequency of change).

User-perceived risk of online applications was operationalized with a three-item reflective construct that included financial, social, and professional risk. Each type of risk was measured on a five-point Likert-scale ranging from not risky to very risky. Four control variables were included in the model, namely type of application, gender, age, and user-perceived computer knowledge.

We coded for five types of applications, namely online banking, gaming, retail, social networking, and student records (see appendix for details about the application scenarios). The applications were selected because of their presumed association with different types of risks. More specifically, we suggest that online banking and retail are associated in particular with financial risk because of the financial data that are an integral part of the applications. Online gaming and social networking are presumably associated foremost with social and professional risk because of the sensitive personal information that is part of these applications. In contrast, we expect student networking to be associated foremost with professional risk because of data that are closely related with a user's career (in addition to

financial data and risk). The appendix provides descriptive statistics of the measurements and inter-item correlations.

4. DATA ANALYSIS AND RESULTS

The data from the survey were analyzed using the structural equation modeling (SEM) approach with Warp3 PLS software that applies the partial least squares (PLS) technique (http://www.scriptwarp.com/warppls). SEM is a second generation statistical method that, in contrast to regression, allows for the simultaneous assessment of multiple independent and dependent constructs, including multi-step paths (Gefen, Straub, & Boudreau 2000). PLS was considered an appropriate method to test the research model because there is a broad agreement among scholars that PLS is well suited for exploratory research and theory development (in contrast to theory testing), which is the case in the current research study. As described above, we conducted two separate analyses, one for each operationalization of password-related efforts (password strength and frequency of change). In both analyses demographic data and risk-perception data were identical, whereas the indicators for password-related effort (strength and frequency) and the associated impacts on intention to use differed.

We tested the research models in two steps (Anderson & Gerbing 1988). In the first step, the quality of the measurement model was assessed by determining its overall fit and testing its factorial validity in the form of convergent and discriminant validity (Gefen & Straub 2005). In the second step, path effects and significance levels in the hypothesized structural model were examined to test the hypotheses. Results from each step are presented next.

Measurement Model

To assess the model fit with the data, it is recommended that the p-values for both the average path coefficient (APC) and the average r-squared (ARS) be both lower than 0.05. In addition, it is recommended that the average variance inflation factor (AVIF) be lower than 5 (Kock 2009). In reference to the results that are presented in Table 2, all of the three criteria are met in both models, and we have reason to assume that the models have acceptable predictive and explanatory quality.

Since our research models have only one construct that contains more than one item (risk) the test of the measurement model is straightforward. To assess the factorial validity of a reflective construct, it is recommended to test for convergent and discriminant validity.

Table 2: Model Fit Indices and P-Values

	Strength-model	**Change-Model**
Average path coefficient (APC)	0.099 p<0.001	0.026 p<0.001
Average R-Squared (ARS)	0.139 p<0.001	0.065 p<0.001
Average Variance Inflation factor (AVIF)	1.005 (good if <5)	1.007 (good if <5)

Convergent validity is the extent to which items are thought to reflect one particular construct (Straub, Boudreau, & Gefen 2004). We assess convergent validity by examining the loadings of the measurement items on the reflective construct and found acceptable results: the loadings of financial risk, social risk and professional risk on the risk-construct were all above the recommended threshold of 0.5 with 0.715, 0.899, and 0.908, respectively, and significance-levels of $p<0.001$ (Hair, Anderson, & Tatham 1987). In contrast, the loadings on all other factors (i.e., cross-loadings) were much lower (<0.2). Both composite reliability and Cronbach's alpha of the risk construct were above the recommended conservative threshold of 0.7 with 0.881 and 0.794, respectively (Fornell & Larcker 1981). Based on these results, we conclude that the three risk-related items exhibit acceptable convergence toward the latent variable of user-perceived risk.

Discriminant validity is the extent to which items reflect their suggested construct differently from the relation with all other items in the measurement model (Straub et al. 2004). Upon examining the correlations among the latent variables we expect to find the square root of the average variance extracted (AVE) to be much larger than any correlation among any pair of latent constructs. Again, we focus on the risk construct where we recorded an AVE of 0.845, and substantially lower correlations (<=0.104) with any other item. Based on these test results, we suggest that the three risk-related measurement items indeed reflect the latent variable of user-perceived risk that differs from all other measurement items in the model.

Structural Model

The next step of data analysis involved examining the structural models in order to test

our hypotheses. The results are presented in Figures 2 and 3, and summarized in Table 3.

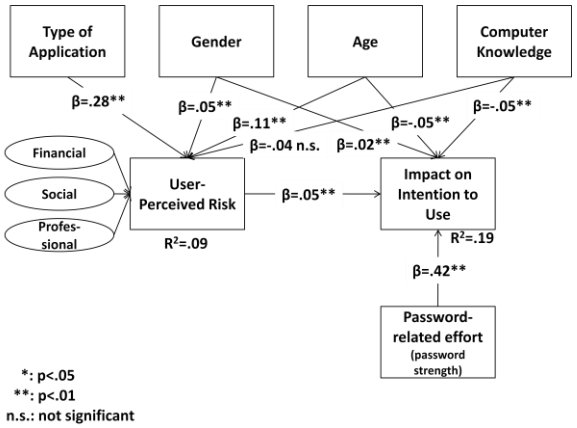

Figure 2: Structural Model for Password Strength

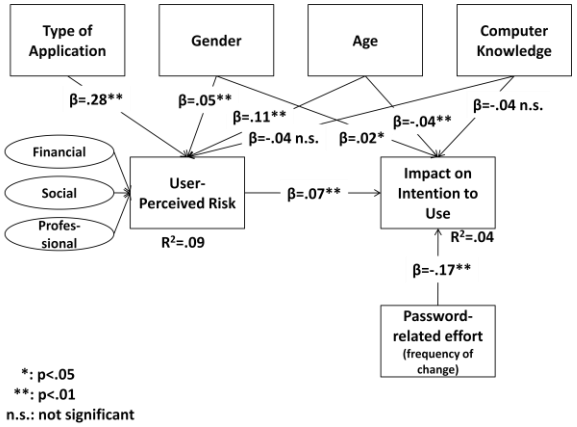

Figure 3: Structural Model for Frequency of Password Change

Table 3: Model Results

Hypotheses	Support for Password Strength	Support for Frequency of Change
H1: Password-related efforts are associated negatively with the intention to use an online application.	No (link is significant, but opposite sign)	Yes
H2: User-perceived risk of an online application is associated positively with the impact of password-related efforts on intention to use an online application.	Yes	Yes

We found links that were significant at the p<.01 level for both hypotheses in the strength- and change-models. In the strength model, however, the expected sign of the relationship between password strength and impact on intention to use (H1) showed a positive instead of the expected negative direction. A look at the estimated functional relationship between password strength and impact on intention to use exhibits an inverted U-shape with a prominent and unexpected upward sloping part (Figure 4).

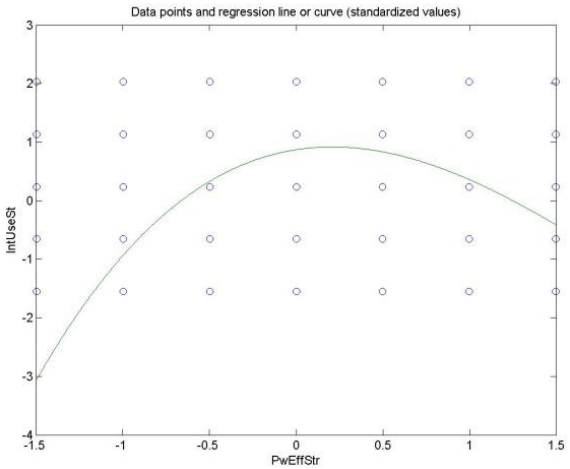

Figure 4: Functional Form between Password Strength (Effort) and Impact on Intention to Use (H1)

In comparison, Figure 5 shows the functional form between frequency of password change and intention to use, which shows the expected linear downward slope.

In contrast, H2 is supported in the correct (upward-sloping) direction for both the strength- and change-models. Still, the coefficients are rather small with 0.05 and 0.07, for password strength and frequency of password change, respectively.

The path coefficients for the remaining control variables are mostly significant (Figures 2 and 3). We note that the type of application exhibits a strong and significant effect on user-perceived risk. The descriptive statistics show that on average financial risk is considered highest for banking and retail, whereas social and professional risk are perceived to be particularly high for social networking applications. The risk associated with online gaming is comparatively lower (Figure 6).

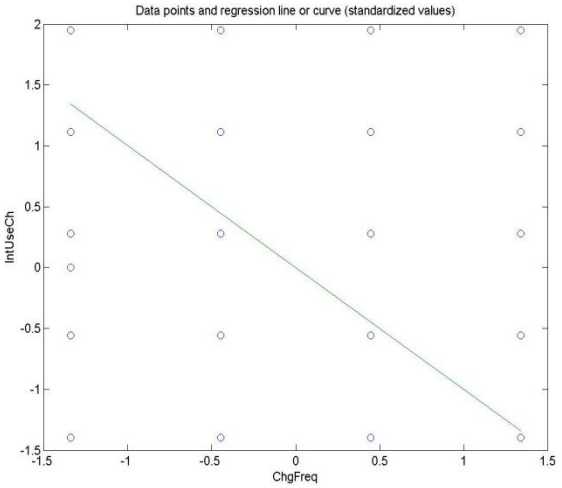

Figure 5: Functional Form between Frequency of Password Change (Effort) and Impact on Intention to Use (H1)

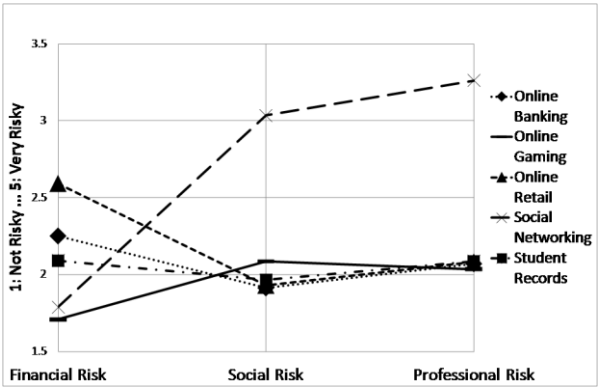

Figure 6: Mean User-Perceived Risk by Type of Application

Gender is significant insofar as female participants indicated both higher user-perceived risk and a higher impact on the intention to use online applications than male participants. Age played a mixed role as both models showed a significantly positive association between age and user-perceived risk and a significantly negative association between age and intention to use. Computer knowledge had only comparatively small (even insignificant) associations with risk and intention to use in both models.

Even though both models have highly acceptable values of fit with the data as reported above, the R-square values are small, in particular for the change model.

5. DISCUSSION

Our data analysis has yielded some interesting results. For efforts related with frequency requirements of password change, the data showed the hypothesized *negative* association between effort and impact on intention to use and the hypothesized *positive* association between perceived risk and impact on intention to use. We interpret the results such that from a user-perspective the inconvenience (=effort) associated with frequent password changes has a negative effect on the intention to use online applications. In contrast, user-perceived risk has a counterbalancing effect, in particular for high-risk applications. This latter insight was obtained by splitting the data sample into high-risk and low-risk groups based on overall perceived risk. While the high-risk group exhibited a strong and significant positive relation with intention to use, the association was non-significant for the low-risk group.

The results differ for password strength, our second measure of password-related efforts. Here, we find a curvilinear relationship between password strength and impact on intention to use that resembles the form of an inverted U, with a prominent *positive* upward slope. The relationship between user-perceived risk and intention to use is *positive* as expected. The results for low- and high-risk groups are very similar, even though the low-risk group again shows a non-significant relationship between risk and intention to use. We interpret the results such that for password strength, the inconvenience factor appears to play less of a (negative) role for intention to use than what we found for the efforts related with frequent password changes. Users appear to be more accepting of the requirements associated with setting up and using passwords that are of medium length and strength, despite the associated effort. Incidentally, with a ratio of explained to unexplained variance (R^2) of 0.19, the strength of the model that uses password strength as its dependent variable is higher than the strength of the model that uses frequency of password change (R^2=0.04).

We also note that our results show no clear symmetry in the reactions of users to password related efforts and application-related risk. Moreover, the relation between effort and user-perceived risk on the one hand and user-reaction on the other hand appears to depend on the operationalization of effort (password strength versus frequency of required change).

6. CONCLUSIONS

The results of our study have implications for practitioners as well as for researchers. Practitioners may be interested in the differences that we found in user reactions regarding the requirements of password strength versus frequency of change. We suggest that in order to be effective, system administrators need to rely more on the inherent strength of password length and character-types, than frequency of password change. In addition we found that the extent to which users are aware of the risks associated with the use of online applications appears to add to the willingness to accept long and complicated passwords, but not necessarily passwords that have to be changed very often.

Our research shows a continued need to increase awareness of the various risks associated with the use of online applications. Users appear to be willing to make security-related efforts in particular to the extent that they help avoid negative implications for their own well-being. We suggest that system administrators need to be careful to combine the need for security from organizational and technical perspectives with the perceptions of the individual user. The results of our study complement established security practices, as they emphasize the need to include individual security perceptions and behavior as part of comprehensive security strategies.

The results of our study also have implications for research, in particular research that applies fit variables (e.g., Goodhue & Thompson 1995). We attempted to identify a clear trade-off between security-related efforts in the form of password requirements and benefits (risk mitigation) that could help us devise guidelines to achieve optimal fit between the two factors. We found, however, that the relationship between both factors can vary for different measures (password length vs. frequency of change), and that the reactions of users to situations of low risk/high security-related efforts (under-fit) were not necessarily the same as the reactions of users to situations of high risk/low security-related efforts (over-fit). The results in the current study support earlier calls to apply an asymmetric approach when studying fit-measures in organizational settings (Gebauer 2009).

One limitation of the study lies in the group of survey participants (undergraduate students) that may not adequately represent the general population, in particular staff employed in a typical business setting. A generalization of our results should therefore be conducted with caution. We suggest a replication of our approach in a more professional setting to confirm and extend our insights. In addition, the current study was exploratory and therefore used rather crude measures to assess password-related efforts. Future studies should apply more granular measurements in order to obtain more refined results regarding the user-perceived tradeoff between efforts and benefits (risk-mitigation). Experimental research designs may be in order to achieve the latter research goal.

In conclusion, our research can help shed light on the interplay between the need to maintain security and the efforts associated with achieving a certain level of security, from a user-perspective. In order to be effective, system administrators and managers need to develop comprehensive strategies to security that balance the needs of the organization with the needs and preferences of the individual user. We think that the insights presented in the current study can help achieve that goal.

7. Acknowledgments

The authors wish to thank the study participants for their time and insights, as well as the Cameron School of Business at the University of North Carolina Wilmington for financial support in the form of a summer research grant to the first author.

8. REFERENCES

Anderson, J., & Gerbing, D. (1988). Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach. *Psychological Bulletin*, 103(3), 411-423.

DeWitt, A., & Kuljis, J. (2006). Is Usable Security an Oxymoron? *Interactions*, (May), 41-44.

Florêncio, D., and Herley, C. (2007). A Large-Scale Study of Web Password Habits. *Proceedings of International World Wide Web Conference*, Banff, Alberta, Canada.

Forget, A., Chiasson, S., van Oorschot, P.C., & Biddle, R. (2008). Improving Text Passwords Through Persuasion. *Symposium on Usable Privacy and Security (SOUPS)*, Pittsburgh.

Fornell, C., & Larcker, D. (1981). Evaluating Structural Equation Models with

Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18(1), 39-50.

Garrison, C. (2006). Encouraging Good Passwords", *InfoSec CD Conference '06*, Kennesaw, ACM.

Gebauer, J. (2009). Functional Forms of Fit: An Asymmetric Perspective. *Proceedings of the Americas Conference on Information Systems*, San Francisco, CA. http://aisel.aisnet.org/amcis2009/311/ (accessed April 9, 2011)

Gefen, D., & Straub, D. (2005). A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example. *Communications of the Association for Information Systems*, 16, 91-109.

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. *Communications of the Association for Information Systems*, 4(article7).

Gehringer, E. (2008). Choosing Passwords: Security and Human Factors. Working Paper.

Goodhue, D., & Thompson, R. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly*, 19(2), 213-236.

Hair, J., Anderson, R., & Tatham, R. (1987). *Multivariate Data Analysis*. New York, NY: Macmillan.

Hart, D. (2008). Attitudes and Practices of Students Towards Password Security. *Consortium for Computing Sciences in Colleges*.

Jones, L., Anton, A., & Earp, J. (2007). Towards Understanding User Perceptions of Authentication Technologies. *Proceedings of the 2007 ACM workshop on Privacy in Electronic Society*, Alexandria, VA, 91-98.

Kline, D., He, L., & Yaylacicegi, U. (forthcoming) User Perceptions of Security Technologies. *International Journal of Information Security and Privacy*.

Kock, N. (2009). WarpPLS 1.0 User Manual. ScriptWarp Systems, Laredo Texas. Retrieved online June 7, 2010 from http://www.scriptwarp.com/warppls/UserManual.pdf.

Kuo, C., Romanosky, S., & Cranor L. (2006). Human Selection of Mnemonic Phrase-Based Passwords. *Symposium on Usable Privacy and Security (SOUPS)*, Pittsburgh.

Lockdown.co.uk (2009). Password Recovery Speeds: How Long Will Your Password Stand up? Retrieved June 7, 2010 from http://www.lockdown.co.uk/?pg=combi.

Neosmart Technologies (2006). *The Advent of Uncrackable Passwords*, 3rd edition. Retrieved online June 7, 2010 from http://neosmart.net/downloads/research/Uncrackable_Passwords.pdf.

Salem, O., Hossain, A., & Kamala, M. (2008). Intelligent Systems to Measure the Strength of Authentication, IEEE Explore working paper.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems*, 13, 380-427.

Weir, Catherine S., Douglas, G., Carruthers, M., & Jack, M. (2009) User Perceptions of Security, Convenience and Usability for ebanking authentication tokens. *Computers & Security*, 28(1-2), 47-62.

Zhao, D.-M., Wang, J.-H., Wu, J., & Ma, J.-F. (2005). Using Fuzzy Logic and Entropy Theory to Risk Assessment of the Information Security. *Proceedings of the Fourth International Conference on Machine Learning and Cybernetics*, Guangzhou, IEEE.

Editor's Note:

This paper was selected for inclusion in the journal as a CONISAR 2010 Meritorious Paper. The acceptance rate is typically 15% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2010.

Appendices and Annexures

Questionnaire

Background

1. Gender (male, female)
2. Age (under 17, 17-18, 19-20, 21-22, 23-24, 25-26, 27-30, 31-35. 36-40, 41-50, over 50)
3. What is your level of general computer knowledge compared to the majority of people your age? (Well Below Average, Below Average, Average, Above Average, Well Above Average)

Online Banking: The next few questions relate to online banking. You are considering an online banking web site. The website allows you to check account balances, transfer funds, pay bills, and interact with customer service representatives.

4. How risky do you perceive the Online Banking scenario to be? (Not Risky, A Little Risky, Moderately Risky, Risky, Very Risky, each with respect to Financial Riskiness, Social Riskiness, Professional Riskiness)
5. Please rate how each of the password change policies would affect your likelihood of using this online banking site. (very negative, negative, indifferent, positive, very positive, each with respect to password must be changed every week, password must be changed every 3 months, password must be changed every year, password never needs to be changed)
6. Please rate how each of the password policies would affect your likelihood of using this online banking website. (very negative, negative, indifferent, positive, very positive, each with respect to no minimum, password can be blank, minimum 4 character password, minimum 8 character password, minimum 12 character password, minimum 4 character, non-letters required, i.e., password must contain characters other than letters, such as (*,$,1-9,!), minimum 8 character, non-letters required, minimum 12 character, non-letters required)

Online Gaming: The next few questions relate to on line gaming web site. You are considering an online gaming web site. The site offers single person games such as solitaire and crossword puzzles. The site allows you to store and manage your personal scores. The site is free.
Questions 7-9 correspond with questions 4-6.

Online Retail: The next few questions relate to on line retail. You are considering an online retail web site. The site allows you to shop for electronic products in the range of $10-$500. You can place orders, pay by credit card, store items you wish to buy in the future, and track your orders.
Questions 10-12 correspond with questions 4-6.

Social Networking Site: The next few questions relate to a social networking site. You are considering an online social networking web site. The website allows you to share pictures, display information about yourself, join groups with common interests, and meet people through shared contacts.
Questions 13-15 correspond with questions 4-6.

Student Records System: The next few questions relate to an online student records system. You are considering using an online student records system. The system allows you to check past grades, check your GPA, change majors, see outstanding account balances, and view your transcripts.
Questions 16-18 correspond with questions 4-6.

Descriptive Statistics and Correlations

	Min	Max	Mean	Std-Dev	1	2	3	4	5	6	7	8a/b
1. Gender	1	2	1.418	.493								
2. Age	2	10	3.529	1.184	-.023**							
3. Computer Knowledge	1	5	3.404	.689	-.109***	-.022*						
4. Application	1	5	n/a	n/a	n/a	n/a	n/a					
5. Financial Risk	1	5	2.091	1.074	.062***	.091***	-.020*	-.038***				
6. Social Risk	1	5	2.189	1.134	.042***	.046***	.004	.127***	.427***			
7. Professional Risk	1	5	2.309	1.191	.035***	.057***	-.013	.148***	.458***	.802***		
8.a Password-related Effort (Password Strength)	1	7	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
8.b Password-related Effort (Frequency of Change)	1	4	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
9a. Intention to Use (impact of password strength)	1	5	2.733	1.117	.031***	-.034***	.019*	.011	.049***	.043***	.033***	.259***
9b. Intention to Use (impact of frequency of password change)	1	5	2.669	1.196	.034**	-.026*	-.012	-.007	.075***	.056***	.050***	-.173***

*: <=0.05

**: <=.01

***: <=.001