NSU Florida
NOVA SOUTHEASTERN UNIVERSITY

Nova Southeastern University
NSUWorks

CEC Theses and Dissertations

College of Engineering and Computing

2016

An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity

Stephen Mujeye
Nova Southeastern University, smujeye@nova.edu

This document is a product of extensive research conducted at the Nova Southeastern University College of Engineering and Computing. For more information on research and degree programs at the NSU College of Engineering and Computing, please click here.

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

Part of the Databases and Information Systems Commons, and the Information Security Commons

Share Feedback About This Item

NSUWorks Citation

Stephen Mujeye. 2016. *An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity.* Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (963) https://nsuworks.nova.edu/gscis_etd/963.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity

by

Stephen Mujeye

A dissertation report submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2016

We hereby certify that this dissertation, submitted by Stephen Mujeye, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Yair Levy, Ph.D.
Chairperson of Dissertation Committee

Date

Wei Li, Ph.D.
Dissertation Committee Member

Date

Herb Mattord, Ph.D.
Dissertation Committee Member

Date

Approved:

Ronald J. Chenail, Ph.D.
Interim Dean, College of Engineering and Computing

Date

College of Engineering and Computing
Nova Southeastern University

2016

SIGNED ORIGINAL ON FILE AT NSU

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity

by
Stephen Mujeye
April 2016

The proliferation of information systems (IS) over the past decades has increased the demand for system authentication. While the majority of system authentications are password-based, it is well documented that passwords have significant limitations. To address this issue, companies have been placing increased requirements on the user to ensure their passwords are more complex and consequently stronger. In addition to meeting a certain complexity threshold, the password must also be changed on a regular basis. As the cognitive load increases on the employees using complex passwords and changing them often, they may have difficulty recalling their passwords. As such, the focus of this experimental study was to determine the effects of raising the cognitive load of the authentication strength for users upon accessing a system via increased strength for passwords requirements. This experimental research uncovered the point at which raising the authentication strength for passwords becomes counterproductive by its impact on end-user performances.

To investigate the effects of changing the cognitive load (via different password strength) over time, a quasi-experiment was proposed. Data was collected in an effort to analyze the number of failed operating system (OS) logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock & reset account). Data was also collected for the above relationships when controlled for computer experience, age, and gender. This quasi-experiment included two experimental groups (Group A & B), and a control group (Group C). There was a total of 72 participants from the three groups. Additionally, a pretest-posttest experiment survey was administered before and after the quasi-experiment. Such assessment was done in an effort to see if user's perceptions of password use would be changed by participating in this experimental study. The results indicated a significant difference between the user's perceptions about passwords before and after the quasi-experiment.

The Multivariate Analysis of Variance (MANOVA) and Multivariate Analysis of Covariate (MANCOVA) tests were conducted. The results revealed a significance difference on the number of failed logon attempts, average logon times, average task completion, and amount of request for assistance between the three groups (two treatment groups & the control group). However, no significant differences were observed when controlling for computer experience, age, and gender. This research study contributed to the body of knowledge and has implications for industry as well as for further study in the information systems domain. It contributed by giving insight into the point at which an increase of the cognitive load (via different password strengths) become counterproductive to the organization by causing an increase in number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account). Future studies may be conducted in the industry as results by differ from college students.

Acknowledgements

I’m grateful to God for allowing me to go through the doctoral journey. I’m thankful for all the blessings He has showered on my along the way and they include putting me in touch with wonderful people.

I’m very thankful for the guidance I received from Dr. Levy. I have learned so much from him during the process. His attention to detail is exceptional and I believe I have become a better person because of his guidance. I could not have asked for a better dissertation committee chair. I’m also thankful to Dr. Herb Mattord and Dr. Wei Li for being wonderful committee members. Your feedback was great appreciated.

I would like to express my appreciation to the administration at McHenry County College for allowing me to conduct my experiment at the college. Dr. Miksa and his team were very supportive and I thank you for that.

I would also like to thank my brother Douglas for inspiring me to get into the program. I spend countless hours with him talking about both my dissertation and the process. Thank you for listening as well as giving advice.

My grandfather, Pastor O. T. Gutu strongly believes in education and he inspired me in so many ways. I’m thankful for his words of encouragement as well as checking on my progress each time I spoke to him.

I’m also thankful to my family for the support they gave me during the process. My wife Precious was a great cheer leader and I’m certainly thankful for her support. My kids, Stephen Jr. Kimberly, and Shevanopa were tolerant during the process and I want to say a special thank you to you all.

May God bless you all.

Table of Contents

Chapters

Appendices

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Harby, Qahwajim, and Kamala (2010) mentioned that security is an important issue for business and one of the main aspects of security is user authentication. Warkentin, Davis, and Bekkering (2004) pointed out that authentication is a foundation procedure when it comes to information system security management. Several authentication methods have been developed over the years including biometric–based methods of fingerprints, face, palm, hand geometry, iris, retina, skin reflection, veins, teeth, and keystroke dynamics (Gearhart, 2010). However, authenticating users using passwords is the widely used method in information systems and on computer networks (Mattord, Levy, & Furnell 2013). Crawford (2013) also confirmed that passwords are a part of life for most individuals as they use them at work and home to secure digital resources.

Sridhar (2010) highlighted the human limitation in processing capacity and recorded undesirable results such as user posting passwords when the password strength was raised. Since passwords are the widely used method, it appears that a need exists to better understand the balance between increased password strength, i.e. improving security, and the complexity requirement placed on users (Carstens, McCauley-Bell, Malone, & Demara, 2004). Therefore, a study investigating the point at which undesirable results begin to happen when the password strength is raised appears warranted. This study provides a deeper insight as well as understanding of the balance in increasing the authentication requirements and at the same time increasing the capabilities of the human mind to recall such complex passwords. The results of this study are helping by providing recommendations for both the research and practice.

Problem Statement

The research problem that this study tackled is the obstacle of password memorability, which is further complicated by the fact that users have many passwords to recall for computers, networks, and Websites among other systems (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005). Wiedenbeck et al. (2005) further noted that passwords have to be constantly changed in order to improve security, which increases the burden on the human mind and makes it difficult for users to remember their passwords. Henry (2007) pointed out that an infrequently used password that must be changed constantly, along with other security countermeasures, increases the cognitive load on users. According to Hogg (2007), “cognitive load is defined as the processing of information that occurs in working memory” (p. 188). Kinsbourne and George (1974) determined limitations to the human memory that affect humans’ ability to recall complex passwords that must be constantly changed. The human working memory has a size that can be verbally rehearsed in about two seconds and that limitation will affect the cognitive ability to recall complex passwords.

Erlich and Zviran (2010) noted the fact that there is an increase in the number of information systems while one of the challenges that come with this increase is information security. One of the essential functions of information security is access control and it deals with who gains control to the system (Hwang, Wu, & Liu, 2000). Kumari and Chithraleka (2012) mentioned that the main objective of access control is the protecting of resources from unauthorized access at the same time ensuring authorized access. One of the prerequisites of access control, at the foundation of information security is authentication, which is responsible for the establishment of the identity of the person attempting to gain access to a system or network. Ren and Wu (2012) defined authentication as the act of confirming that the communicating entity is the one claimed. Levy, Ramim, Furnell, and Clarke (2011) noted that “User authentication is the process of verifying an attempted request of an individual (i.e. “the user”) to gain access to a system” (p. 104). Menkus (1998) stated that methods of user authentication can be dichotomized into three main categories:

- Knowledge-based authentication – what the user knows
- Possession-based authentication – what the user has
- Biometric-based authentication – what the user is

From these three categories, the most widely used method of user authentication is knowledge-based authentication. According to Erilich and Zviran (2009), knowledge-based user authentication can be further divided into different categories, which include (a) character-based, (b) image-based, and (c) question/answer-based.

Passwords are in the question/answer-based category and are the most used method of authentication in information systems (Kim, 2012). Dasgupta and Saha (2009) noted that one of the main ways used to authenticate users is through the use of passwords and this is when the user confirms their identity with a secret key. In order for the passwords to be effective, they need to be complex and resist several types of password attacks (Tsai, Lee, & Hwang, 2006).

Passwords, by their nature, are vulnerable to attacks like “dictionary attacks” and “brute force attacks” (Molloy & Li, 2011). A dictionary attack is a malicious event where an attacker builds a database populated with various combinations of possible passwords, which are referred to as “the dictionary” (Chakrabarti & Singha, 2007). The attacker then attempts to logon to the system using the passwords from that database; if one password fails, the attacker proceeds to the next one until all options in the database have been exhausted or the system locks out. Such process can be automated using code to expedite the attack trails including common time delay to overcome system lockouts. Dictionary attacks can be either offline dictionary attacks, if they are non-interactive or online dictionary attacks if they are online and interactive. Medlin and Cazier (2007) described the brute force attack as an attack that occurs when every possible combination of letters, numbers, and symbols are used in an effort to guess a password. Oreku and Li (2009) also referred to the password as the frontline of defense against attackers and that virtually every system uses the password as a method of authenticating users. Despite this, passwords have many limitations. Meng (2012) pointed out that passwords suffer from security and usability problems. Because users have limitations in long-term memory, they tend to use short passwords that are easy to remember (Vu, Proctor, Spantzel, Tai, Cook, & Schultz, 2006). The use of short and easy-to-remember passwords presents a security risk to the organization from attacks like brute force attack (Zviran, & Haga, 1999). Consequently, it is important for users to avoid using simple dictionary words and to use complex passwords. In order to prevent users from using weak passwords, organizations create password policies (Shay, Komanduri, Kelly, Leon, Mazurek, Bauer, Christin, & Cranor, 2010). Inglesant and Sasse (2012) pointed out that password policies dictate the minimum number of characters, complexity, expiration limits, and/or the number of times a user can reuse the same password. There is, therefore, great need to improve password security as well as investigate the balance between password complexity and users' productivity (Carstens et al., 2004). However, when the passwords requirements are too complex, that may create a situation in which the user forgets their password and that can have a negative effect on productivity as well as task completion (Herley, 2009). In situations where users forget their passwords and contact the help desk, time and resources will be wasted as help desk staff reset the password, or if the help desk is closed, users must wait until the following business day in order to reset their password, which further reduces corporate productivity (Shay & Bertino 2009). Duggan, Johnson, and Grawemeyer (2012) further stated that the benefits of using complex passwords are unclear or very small. The claim above is confirmed by "productivity paradox" in which Nobel Laureate Rober Solow stated that there is discrepancy between Information Technology (IT) investments and productivity output (Wong & Dow, 2011). IT productivity paradox examines the efficiency of IT in changing inputs to outputs; examples of input are hardware investments, IT capital and expenditures while output examples are profitability, revenue and market value (Marthandan & Meng, 2010). Time and resources used by the help desk staff fit into the category of inputs. Mittal and Nault (2009) pointed out that evidence of the impact of investments in IT and performance seems to elude researchers as well as investors.

Shay et al. (2010) pointed out that while strong password policies improve information security, there is a challenge that those users may have a difficult time remembering the passwords. Novakovic, McGill, and Dixon (2009) claimed that the use of strong passwords and constantly changing them can have counterproductive effects as it places too much cognitive load on the users. As the cognitive load increases, it may result in users taking time away from performing other job functions, as well as increasing help desk and IT support time with requests to reset passwords (Brostoff & Sasse, 2000).

The Cognitive Load Theory (CLT) is based on cognitive science, which equates the human mind to a processing system with working memory and storage memory (Sweller, 1988). Information that humans receive is stored in the long-term memory after working memory processes it. Miller (1956) mentioned that the working memory is limited in such a way that the human mind can only hold seven items simultaneously, seven items translate to 23 bits of information. Hogg (2007) further stated that working memory is limited and that makes it difficult for humans to process complex tasks. The limitations of the user's memory can affect the ability to remember complex passwords (Boechler, 2006). Novakovic et al. (2009) also pointed out that when users are required to constantly change complex passwords, it appears to place a high cognitive load on them. Novakovic et al. (2009) outlined the characteristics of a complex password in their research; however, users were not actually given the opportunity to change the passwords as they simply completed online surveys. The scenario given to users mentioned a 12-character password changed every 30 days but did not involve changing the password strength.

Passwords remain the most widely used authentication method in information systems and additional research in keeping the authentication method strong without increasing the user's cognitive load is needed (Henry, 2010). Even though other authentication methods such as the image-based have been developed, passwords remain the viable alternative for the majority of information systems (Chiasson, Forget, Stobert, van Oorschot, & Biddle, 2009). Therefore, additional research to address the problem of increasing password authentication strength seems highly warranted.

Research Goals

The main goal of this study is to assess the effect of changing the cognitive load (via different password strengths) over time on the number of failed operating system (OS) logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock & reset account), as well as assess the aforementioned relationships when controlled for age, gender, and computer experience. This study will also assess the point at which raising the password strength becomes counterproductive. Significant differences on the number of failed OS logon attempts, users' average logon time, average task completion, and number of requests for assistance will be used to determine the point at which raising the password strength becomes counterproductive. The need for this work is demonstrated by previous studies (Keith, Shao, & Steinbart, 2007; Novakovic, McGill, & Dixon, 2009) that highlighted memorability and performance problems with long passwords. Keith, Shao, and Steinbart (2007) carried out an experimental study in which one of the groups was required to have a complex 15-character password. Their results indicated that the group with a complex password experienced a high rate of unsuccessful logins due to the users forgetting their passwords. However, their study did not manipulate the cognitive load of the user's passwords. In their work, Novakovic et al. (2009) acknowledged that passwords are the main way of authenticating users as well as the fact that they need be strong. They also pointed out the challenge of increasing password security, which results in the negative impact it has on usage. Cahill, Martin, Phegade, Rajan, and Pagano (2011) also demonstrated how increasing password complexity requirements can lead to problems when users have hard times keeping up with the requirements.

This study builds on previous research by Sasse, Brostoff, and Weirich (2001) in which they pointed out human memory limitations with passwords have an impact on information security. Mihajlov and Blazic (2011) also pointed out that as authentication mechanisms like passwords increase in complexity, the probability of mistakes significantly increases due to the load placed on the human mind. Shay et al. (2010) performed some work in an effort to find how password policies can be improved in a way that does not negatively impact their use by users. They concluded that some users struggle to comply with new password requirements with over 10% going to the help desk after forgetting their passwords. Their work was based on a paper-based survey and did not have the ability to measure when the password policies actually begin to be counterproductive. In this proposed study, users will have their password strength increased and the effects will be observed.

This proposed research is based on previous studies, such as Grawemeyer and Johnson (2011) that highlighted the fact that current information security policies do not take into account the cognitive load placed on users as they have to maintain several passwords. This proposed research builds on the work by Zviran and Haga (1999), which confirmed the point that frequently changing a password hinders both memorability and recall.

Research Question

The main research question that this study will address is: At what point does the increase of the cognitive load (via different password strengths) become counterproductive to the organization by causing an increase in number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account)? At what point does such increase become counterproductive to the organization when controlled for age, gender, and computer experience?

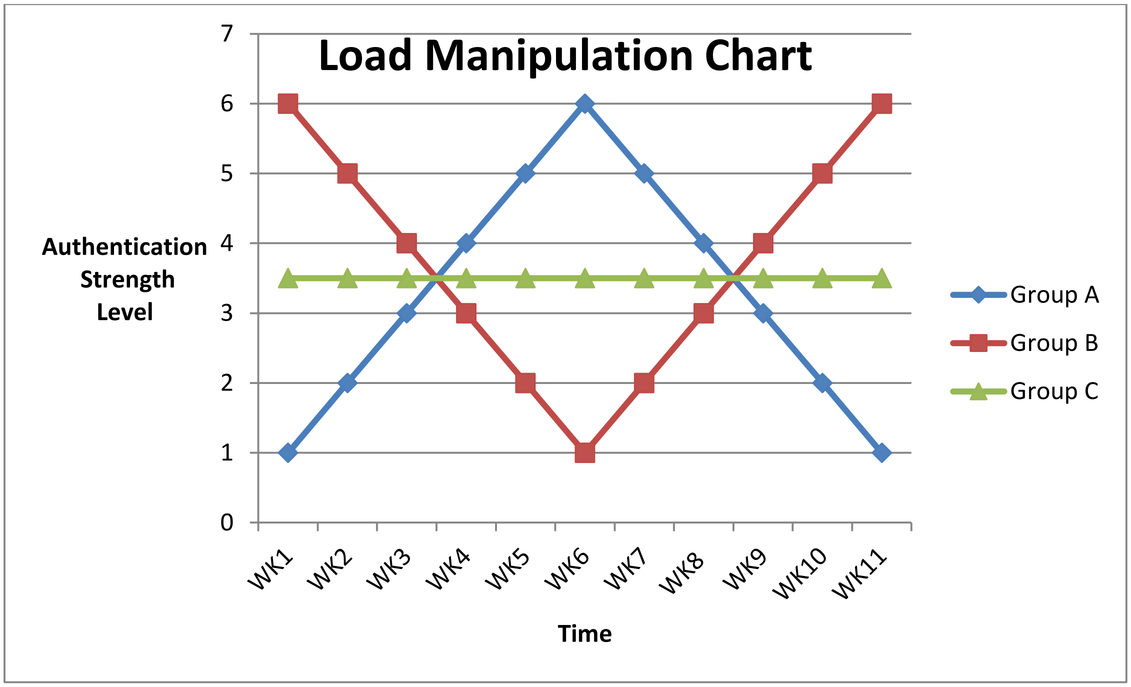


Figure 1: Load Manipulation Chart

Figure 1 shows how the authentication strength will be manipulated throughout the experiment period of 11 weeks.

To measure the effects of increasing password strength, a system will be set up and all three groups will be asked to logon to the system. The three groups will be Group A (increase-decrease password strength), Group B (decrease-increase password strength), and Group C (fixed password strength). Once logged in, the users will be asked to perform specific functions. The system will track the following four measures: a) average number of failed OS logon attempts for all the three groups, b) the average time it takes for each user to logon to the system, c) the average time they will take to complete specified tasks to emulate workplace tasks, and d) the number of request for assistance (unlock and reset account), if any. Each of the four performance measures above will be controlled for age, gender, and computer use experience.

McCloskey and Leppel (2010) concluded that age has an impact on how users participate in electronic activities. In their study, they grouped their subjects into three age groups, young (18-25), mature (50-69), and elderly (70 & up). While the study by McCloskey and Leppel (2010) did not include the 26-49 age groups, it was important in pointing out differences among older and younger adults when it comes to using technology. This research study will investigate whether differences in age play a factor on user's activities when the cognitive load (via different password strengths) is changed over time. Awwal (2012) pointed the need to measure specific consumer groups following a research which showed different study results based on age and gender. The need to measure based on gender was validated by Banerjee, Kang, Bagchi-Sen, and Rao (2005), they concluded that there are different behaviors among males and females when using Internet services. The performance measures in this proposed study will also be controlled for computer use experience. Hoxmeier, Nie, and Purvis (2000) listed experience with electronic communications as one of the most important direct factor that affect user confidence and effectiveness when performing computing operations. The following hypotheses are presented based on the research goals (noted in null layout):

H1: There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H1a: There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.

H1b: There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.

H1c: There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.

H2: There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H2a: There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.

H2b: There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.

H2c: There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.

H3: There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H3a: There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.

H3b: There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.

H3c: There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.

H4: There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H4a: There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.

H4b: There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.

H4c: There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.

Relevance and Significance

This study is relevant as it seeks to gain a better understanding of how changes in cognitive load, via increased password strength, affect number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account). This is supported in the literature based on a survey conducted by Novakovic et al. (2009) who measured how users use their passwords and also pointed out that demanding a user to frequently change passwords places too much cognitive load on users. There have been several research studies on factors that must be considered for users to create strong passwords as well as behaviors which force individuals to create strong passwords (Crawford, 2013, Novakovic et al., 2009). Several studies have also pointed out that the use of strong and complex passwords places a huge cognitive load on users (Herley, 2009; Shay et al., 2010). However, a review of literature revealed few studies have focused on the time at which the password strength increase becomes counterproductive to the organization by causing an increase in number of failed OS attempts, users' average login times, average task completion times and number of request for assistance (unlock and reset account).

This research will be significant in that it will add to the body of knowledge regarding the effects of changing the cognitive load (via different password strength) over time. Passwords remain the widely used method of authentication (Kim, 2012) and this study will add insight to the widely used method.

Barriers and Issues

One of the barriers will be to have students get comfortable accessing computers in the virtual environment. To mitigate this problem, a comprehensive training of using Oracle VM VirtualBox will be held in the first two weeks of the semester. Another issue will come from students who may choose not to logon to their computers after the instructions are given and they will not be included in the data.

Limitations

This experiment will be conducted at a medium sized two-year community college and participants will be undergraduate students pursuing an Associate degree. Additional studies will be required to replicate the findings at other colleges and institutions as well as in industry.

Definition of Terms

Access control policy- A definition of how a system should provide or deny access (Kane & Browne, 2006).

Audit log – a log that can track user authentication attempts (Ciampa, 2012).

Audit records – logs that are the second most common type of security-related operating system logs (Ciampa, 2012).

Authentication - "the act of confirming that the communicating entity is the one claimed" (Ren & Wu, 2012, p.714).

Brute force attack – an attack that occurs when every possible combination of letters, numbers, and symbols are used in an effort to guess a password (Medlin & Cazier, 2007).

Cognitive load- "the processing of information that occurs in working memory" (Hogg, 2007, p.188).

Cognitive Load Theory (CLT) – based on cognitive science which equates the human mind to a processing system with working memory and storage memory (Sweller, 1988).

Dependent variable - "the variable affected by the independent variable; for example, the outcome" (Trochim & Donnelly, 2008, p. 8).

Dictionary attack - a malicious event where an attacker builds a database populated with various combinations of possible passwords (Chakrabarti & Singha, 2007).

Independent variable - “the variable that you manipulate. For instance, a program or treatment is typically an independent variable.” (Trochim & Donnelly, 2008, p. 8).

Information security – the tasks of securing information that is in a digital format (Ciampa, 2012).

Password – in the question/answer-based category and are the most used method of authentication in the information systems (Kim, 2012).

Password policies – dictate the minimum number of characters, complexity, expiration limits, and/or the number of times a user can reuse the same password (Inglesant & Sasse, 2012).

Multivariate analysis - “statistical analysis that involves more than one dependent variable” (Mertler & Vannatta, 2010, p. 345).

Network–a group of computers and other devices that are connected by and can exchange data via some type of transmission media, such as cable or wirelessly (Dean, 2010).

Security – confidence that a given approach will produce dependable and intended outcomes (Shoemaker & Sigler, 2014).

System – a collection of mutually supporting and interacting components designed to accomplish a given purpose (Shoemaker & Sigler, 2014).

User– a person who uses a computer (Dean, 2010).

User authentication - “the process of verifying an attempted request of an individual (i.e. “the user”) to gain access to a system” (Levy, Ramim, Furnell, & Clarke, 2011, p. 104).

Validity - “the best available approximation of the truth of a give proposition, inference, or conclusion” (Trochim & Donnelly, 2008, p. 14).

Summary

Chapter one provided an introduction to this study, identify the research problem, discuss the relevance and significance of conducting this study, as well as to provide a theoretical basis for this study. The research problem this study will address is the obstacle of password memorability, which is further complicated by the fact that users have many passwords to recall for computers, networks, and Websites among other systems. Valid literature supporting the need for this research was also presented. Moreover, chapter one also presented the main goal and main research question that will be addressed through this study. The main goal is to assess the effect of changing the cognitive load (via different password strengths) over time on the number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account), as well as assess the aforementioned relationships when controlled for age, gender, and computer experience. The main research question that this study will address is: At what point does the increase of the cognitive load (via different password strengths) become counterproductive to the organization by causing an increase in number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account)?

Chapter 2

Review of the Literature

Introduction

In this section, a brief literature review is presented for areas and theories that provide a foundation of this study. The main areas are authentication, password security, and cognitive load theory. The literature review will include the four characteristics noted by Levy and Ellis (2006), they are: a) methodologically analyze and synthesize quality literature, b) provide a firm foundation to a research topic, c) provide firm foundation to the selection of research methodology, and d) demonstrate that the proposed research contributes something new to the overall body of knowledge or advances the research field's knowledge-base.

Authentication

Authentication in general has been around for centuries, however, its use in the computer industry dates back to the early 1900 with the use of the Enigma Cipher Machine (Crawford, 1992). Computer authentication using the password method was used in the 1970s with the UNIX operating system, the first widely used operating system in a network environment (Henry, 2007). Authentication is a requirement in any system, Kline, He, and Yaylacicegi (2011) pointed out that this is a process when the identities of participants are verified, the typical way this process is accomplished is with a username and password. Authentication is the second step in the access control mechanism and other steps are identification, authorization, and accountability (Whitman & Mattord, 2016). Huang, Xiang, Bertino, Zhou, and Xu (2014) noted that authentication is an interactive process, which takes place between a user and an authentication server, the authentication process can be summarized as follows:

1) The user first sends out an authentication request

2) The authentication server responds with a challenge

3) The user provides their identity by calculating a response which is validated by the server.

Warkentin, Davis, and Bekkering (2004) noted that authentication is at the foundation as it relates to information system security management. On one hand, Ren and Wu (2012) defined authentication as the act of confirming that the authenticating entity is the one claimed. On the other hand, Levy et al. (2012) mentioned that "User authentication is the process of verifying an attempted request of an individual (i.e. "the user") to gain access to a system" (p.104). Authentication can be achieved in different methods including biometric-based methods and keystroke dynamics (Gearhart, 2010). Menkus (1998) described three categories of user authentication and they are a) knowledge-based authentication - what the user knows, b) possession-based authentication – what the user has, and c) biometric-based authentication – what the user is. Passwords fall into the knowledge-based authentication category and they are the mostly used method in information system (Kim, 2012). The three categories of authentication are discussed below.

Something the User Is (Biometrics)

Choi, Lee, Kim, Jung, and Won (2014) defined biometrics as the quantifiable data related to human characteristics and traits. Hussein and Nordin (2014) took it a step further by describing a biometrics system as "the use of physiological or biological features to recognize the identity of an individual" (p. 1389). Ngugi and Kamis (2013) mentioned that adding a biometric layer is one way of making authentication systems stronger. Two options were suggested, the first option is the physical biometric which relies upon some unique physical characteristic and a second option of behavioral biometrics based on user behavioral patterns. Examples of physical biometric technology include fingerprint, face recognition, DNA, palm prints, hand geometry, iris, and retina while an example of behavioral biometric technology includes typing-pattern biometric or keystroke. Revett (2009) defined keystroke as a behavioral biometric modality monitoring the way user's type on the keyboard. Hussain and Alnabhan (2014) further noted the basic idea of keystroke dynamics as being based on the assumption that people type in uniquely different characteristic manners and the keystroke method depends on the assumption of identifying users certain habitual typing rhythm patterns.

While biometrics-based authentication have the advantage that they are very difficult to copy, share, forge or distribute, they also have some limitation (Choi et al., 2014). The limitations are that biometric technology is expensive to purchase, objectionable to users because of a feeling of invasiveness, has the potential of users giving up some privacy as well as making users vulnerable to unauthorized use of their patterns (Ngugi & Kamis, 2013). Marnell and Levy (2014) also listed that biometric technology several problems that are both technical and behavioral, the problems include data degradation as well as variances in data recorded. Sayoud (2011) listed the following as the main social and ethical problems with biometrics:

- Limitation of freedom
- Loss of privacy
- Risk of imposture
- Risk of false rejection

Something the User Has (Security Token)

Another method users can authenticate is by using something they have, this can be an unclonable device with the ability to store cryptographic key such as a smartcard, RFID tag or a token generator (Dossogne & Lafitte, 2013). For the RFID, Lehtonen, Michahelles, and Fleisch (2007) mentioned that it can be categorized into three sections which are: a) what the product is (object-specific features-based authentication), b) what the product has (tag authentication), and c) where a product is (location-based authentication).

Jung, Choi, Lee, Kim, and Won (2014) observed that one of the limitation of smart cards is that they can be stolen. Choi, Lee, Kim, Jung, and Won (2014) reported that confidential information stored in a smart card can be extracted by physically monitoring power consumption and that when a card is stolen, it can be analyzed by the attacker.

Something the User Knows (Passwords)

The password-based authentication method is the widely used method of authentication, Choi et al. (2014) pointed out that passwords provide a simple and convenient way to authenticate users before providing them with services of a computing or communication system. Table 2 below shows MIT's CTSS computer, which is believed to be the first computer to use the password authentication method in 1962 (Corbató, Merwin-Daggett, & Daley, 1962; Maguire & Renaud, 2012).

Figure 2: CTSS Computer (http://www.wired.com, 2012)

Several studies have confirmed that passwords are the most used method of authentication in information systems (Kim, 2012; Dasgupta & Saha, 2009). When it comes to the group of Web-based serviced systems, useID/password remain the mostly used mechanism for achieving identification and authentication (Banyal, Jain, & Jain, 2013). From the three categories of authentication discussed above, passwords were selected as the basis for this study because of their widespread use. While many alternatives and enhancements to password including the two-factor authentication scheme have been proposed, they have limited use and come with usability issues (Herley, Oorschot, & Patric, 2009). Crawford (2013) pointed out that while passwords have their limitations as an authentication method, there is a strong focus to build systems that rely on users creating and maintaining passwords. Medlin (2013) cited one of the reasons why the password authentication methods remains popular when compared to other authentication methods as its ability to give users quick access into the system. The password remains the widely used method of authentication ahead of biometric and smart card because the latter two continue to have challenges with deployability, privacy, and usability (Czeskis et al., 2012; Ma & Feng, 2011; Wang et al., 2014). It is also worth noting that the password authentication method remains the leading authentication method despite that other alternatives have been explored for decades (Wang et al., 2014).

Table 1: Summary of Literature for Authentication

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
Banyal, Jain, & Jain, 2013	Theoretical		Multi-factor Authentication	A user authentication system that seek to establish specific level of security or users to meet their dynamic of security levels for cloud computing.
Choi et al., 2014	Practical Evaluation		Biometric Scheme Analysis	Adding secret information to the registration,

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				login and authentication phases may help a biometric scheme to overcome security problems.
Czeskis, Dietz, Kohno, Wallach, & Balfanz, 2012	Theoretical		Second factor authentication	An authentication scheme which uses oportunistic identity, an assertions which allow the server to treat logins differently based on how the user was authenticated – allowing the server to provide tiered access or restrict dangerous functionality was proposed.
Dasgupta & Saha, 2009	Empirical Study via Experiments	50,000 Test Accounts	Biologically – inspired authentication technique	A non-obvious bio-inspired too for user authentication can create a protection shield to filter

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				out invalid access requests.
Dossogne & Lafitte, 2013	Theoretical		Authentication Alternatives	Alternatives to the three well know authentication methods were proposed with the aim of protecting the prover against rubber-hose cryptanalysis.
Gearhart, 2010	Case Study		Biometric Authentication	A password that is biometric authentication device was suggested as a way of remote proctoring students. The device ensures integrity as well as alleviating the concerns of educators and accrediting agencies among others.
Kim, 2012	Empirical Study via Questionnaire	70 participants	Password Questionnaire	A keypad which increases the time required for brute force attacks by the finder through formation of random buttons, random button

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
				arrangement and display delay time was suggested for smartphones.
Kline, Ling, & Yaylacicegi, 2011	Empirical Study via Survey	135	Survey formulated based on demographic information, basic technological literacy, and password habits	Users tend to use the common passwords across multiple accounts.
Lehtonen, Michahelles, & Fleisch, 2007	Literature Review and Synthesis		RFID-Based Authentication	The level of security of any RFID-based product authentication application is determined by how it fulfills the derived set of functional and nonfunctional requirements.
Levy et al., 2012	Empirical Study via Experiment	163 participants	Multibiometrics Authentication	Learners are significantly more willing to provide their biometric data and intend to use multibiometrics when provided

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
				by their university compared with same services provided by a third-party vendor.
Marnell & Levy, 2014	Empirical Study via Survey	150	Multibiometric Authentication	This work-in-progress study is anticipated to provide greater understanding and contribution to the field of Information Security in the context of higher-education in two significant ways.
Menkus, 1998	Literature Review		Password Use	A problem exists with various password schemes and that is they offer limited password security.
Ren & Wu, 2012	Theoretical		Authentication Scheme	An authentication scheme which uses hash functions and exclusive –or operations as underling cryptographic

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				primitives was proposed.
Sayoud, 2011	Case Study		Biometrics Technology	The main disadvantage of biometric authentication systems is their potential to locate and track people physically.
Warkentin, Davis, & Bekkering, 2004	Empirical Approach	352	Password Survey, Technology Acceptance Model	Users perceive password procedures to be equally useful regardless of the specific procedure used.

Password Security and Strength

The password authentication method was the earliest user authentication mechanism used on the Internet and it remains the most common mechanism to date (Yu, Wang, Mu, & Gao, 2014).Several research studies confirmed that passwords are the main way used to authenticate users in information system (Mattord et al., 2013; Dasgupta & Saha, 2009). Oreku and Li (2009) mentioned that passwords form the first line of defense against attacks and that almost every system uses passwords for authentication. Passwords are vulnerable to different attacks, which include “dictionary attacks” and “brute force attacks” (Molly & Li, 2011). Passwords also have limitations and they suffer from security as well as usability problems (Meng, 2012). Security issues arise from users creating short and easy-to-remember passwords (Zviran & Haga, 1999). To help address the passwords problems of phishing scams, Trojan horses, and shoulder surfing attacks, Xiao, Li , Lei, and Vrbsky (2014) proposed a differentiated virtual password mechanism which gives the user the freedom to choose a virtual password scheme ranging from weak security to strong security. Xiao et al. (2014) acknowledge that a tradeoff between security and complexity is required since simplicity and security conflict each other. Wang and Wang (2008) also attempted to solve the problems surrounding password by proposing neural networks, however, neural network have proved to have several limitations which include lengthy training time and the arbitration in authentication.

Biddle, Mannan, Oorschot, and Whalen (2011) pointed out that text passwords remain ubiquitous, even though there have been endless criticism, they also noted that passwords will continue to dominate user authentication in the future. In another effort to address the limitations with passwords, Biddle et al. (2011) introduced the object-based password (ObPwd) scheme as a mechanism to generate passwords. The premise for ObPwd is that many users currently possess a large collection of digital content like phots, audio recordings, and videos, ObPwd would then generate a password from such items by computing a hash form the user-selected object then converting the hash bit string to an appropriate password format. Users would only need a strategy to remember which password object they chose.

Some of the security issues with passwords can be solved by creating and implementing password polices (Shay et al., 2009; Inglesant & Sasse, 2012). The characters of a password policy are length character sets, complexity, expiration limits, and the number of times a user can reuse the same password. To ensure different passwords are being used when the time to change comes, the Levenshtein distance can be used as it measures the extent to which two strings differ (Rane & Sun, 2010). Bard (2007) recommended a distance of five or greater in the Damerau Levenshtein distance metric to be considered for maximum strength. Medlin (2013) noted that the first guidelines in creating a good password which was published by the Department of Defense in 1985 is still relevant today, the guideline recommends that:

a) Passwords must be memorized;
b) Passwords must be at least six characters long;
c) Passwords must be replaced periodically;
d) Passwords must contain a mixture of letters (both upper and lowercase), numbers, and punctuation characters.

Crawford (2013) pointed out that when encouraging the use of strong passwords formal controls may be utilized during the creation process, the controls include requiring characteristics. Organizations in healthcare are required to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which also require the use of strong password policies and procedures by security and privacy administrators (Cassini, Medlin, & Romaniello, 2008). Many researchers in IS are in agreement that good password policies help to improve security, however, it is also important for organizations to implement a security policy training to users as that can also help in improving secure behavior (Jenkins, Durcikova, & Burns, 2013). The characteristics of a password policy with some examples are noted in Table 1 (Inglesant et al., 2012).

Table 2: Characteristics and Examples of Password Policy

Characteristic	Example
Length	7-8 Characters
Character Sets	At least one character from three of four classes; Character classes are uppercase letters, lower case letters, digits, and non-alphanumeric characters
Expiry	180 Days
History	Must not be similar to previous 12 passwords

Password policies require users to frequently change their passwords in an effort to improve security, however, places a burden on the human mind and make it difficult for users to remember passwords (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005). Kline, Ling, and Yaylacicegi (2011) expressed that a password policy which increases password length may appear to increase security but may be less convenient to the user and can lead to unsecure behaviors like wring the password down. On the other hand, Warkentin et al., (2004) found out after conducting an empirical study that users perceive easy-to-remember passwords as easier to use than high security passwords and are inclined to use them in the event that a password policy does not exist.

Writing about the characteristics of password strength, Mattord (2012) mentioned the characteristics of a strong password as the effective password length, use of numbers, special characters, and case shifting. Medlin and Cazier (2007) used the same characteristics, however, they also included the ability to enforce changing a password on a regular basis as well as forcing users to use a different password from any password previously used. Mattord (2012) conducted a study in which one of the goals was to identify a means to assess the methods used by Web-based Information Systems to control the strength of passwords used in those systems. Mattord (2012) further identified self-generating password tools that can provide a user with a visual or verbal assessment of the strength of the password. The tools are The Password Meter, Google Password Strength Measure, and the Microsoft Password Checker. The characteristics listed above will be incorporated into the password strength for passwords used by all three groups in this proposed study.

Table 3: Summary of Literature for Password Security and Strength

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
Cassini, Medlin, & Romaniello, 2008	Investigative Study		Regulatory Laws	The US Congress and Federal Trade Commission and other government agencies are making an attempt to address privacy and information security through legislation.
Crawford, 2013	Empirical Study via Survey	218	Password Survey	Controls used during the password creation process shape password strength, however, behavior controls do not produce significantly stronger passwords that informal controls.
Dasgupta & Saha, 2009	Empirical Study via Experiments	50,000 Test Accounts	Biologically – Inspired Authenticatio n Technique	A non-obvious bio-inspired too for user authentication can create a

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				protection shield to filter out invalid access requests.
Jenkins, Durcikova, & Burns, 2013	Empirical Study via Experiment	238	Security Training	Training presented with low extraneous stimuli improves secure behavior more that training presented with high extraneous stimuli
Inglesant & Sasse, 2012	Case Study	196 passwords	Password Use	In addition to maximizing password strength and enforcing frequency, password policies should be designed using HCI principles to help users set appropriately strong password in a specific context of use.
Kline, Ling, & Yaylacicegi, 2011	Empirical Study via Survey	135	Survey formulated based on demographic information, basic technological literacy, and password habits	Users tend to use the common passwords across multiple accounts.

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
Mattord, 2012	Case Study	20 participants	Password Survey	A password that is meaningful to the end user is easier to recall even if it contains additional characters.
Mattord et al., 2013	Empirical Study via Survey Developmental Study	40 Web-based systems	Web-based Authenticatio n	It appears that the authentication methods by Web-based IS measured in the study are not insufficient as compared to current practices in the industry.
Medlin, 2013	Empirical Study via Survey	118	Password Survey	It is important for users to stay vigilant in protecting the information within a network and not just rely on computerized systems.
Medlin & Cazier, 2007	Empirical Analys	90	Password Strength	There is need for health care organizations to provide password education and training in or order to meet regulatory standards.

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
Meng, 2012	Lab Study	42 participants	Graphical Password Authentication	A two-step authentication scheme using image selection and secret drawing was selected.
Molly & Li, 2011	Comparative Analysis		Password Authentication	An adversary requires a small number of challenge-response pairs before the user's password may be uniquely identified and other security options such as decoy digits are catalysts for brute force attacks.
Oreku & Li, 2009	Literature Review and Experimental Study via Experiment		Password Authentication	A one-time password is particularly effective against guessing attacks because even if a password is guessed, it may not be reused due to the time limitations.
Shay et al., 2010	Paper Survey	450 participants	Password Handling, composition, storage, and reuse	The use of stronger passwords causes users to struggle to comply, reuse passwords as

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
				well as to write them down.
Warkentin, Davis, and Bekkering, 2004	Empirical Approach	352	Password Survey, Technology Acceptance Model	Users perceive password procedures to be equally useful regardless of the specific procedure used.
Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005	Experimental Design	40 participants	Alphanumeric and Graphical Password	Graphical password users were able to create passwords with easy but they had more difficulty learning their passwords that alphanumeric users.
Zviran & Haga, 1999	Empirical Study via Questionnaire	36 participants	Password Usage	Users tend to violate secure password practices resulting in passwords that are easy to guess an therefore organizations should have a set of guidelines for selecting implementing passwords.

Cognitive Load Theory

Hogg (2007) defined cognitive load as the processing of information that occurs in working memory. Sweller (1988) stated that the Cognitive Load Theory (CLT) is based on cognitive science which equates the human mind to a processing system with working memory and storage memory. The working memory, which humans rely on to perform tasks like remembering passwords, has limitations, Miller (1956). Storage memory, which can also be referred to as long term memory represents the subconscious storage of items (Sweller, 1988). Sweller, (1988) further noted that long term memory is long term memory is organized into schema which can be accessed by the working memory. As the amount of information that has to be processes increases, the cognitive load also increases leading to users suffering from information anxiety as a result of excessive demands (Fan & Lei, 2008). Studies such as Crawford (2013), Henry (2007), Sridhar (2010), and Shay et al. (2010) support the claim that the use of strong passwords as well as constantly changing them places a high cognitive load on users. Crawford (2013) also noted that strong password requirements can place a heavy burden on users, potentially producing end users goals that significantly different from those implementing the strong password requirements. Shay et al. (2010) pointed out that while password policies result in stronger password, they place a high cognitive load on the user and make it difficult for the users to remember the password. Carstens et al. (2004) in their experimental study mentioned that using complex passwords places a cognitive overload on the users and as result of that users end up having a hard time to remember to passwords. The use passphrases, which consist of several words, have been suggested as being secure, however, users of passphrases have experienced unsuccessful logins because of memory recall failure (Keith et al., 2009). Passwords which are too long to be managed in short memory may be too difficult for users to memorize which can possibly lead to users writing the passwords down (Keith et al., 2009). Shay et al. (2010) agreed that the high cognitive load further leads to undesirable and unsafe practices like reusing the password or writing the password down. Carstens et al. (2004) noted the need to better understand the balance of improving password security and the complexity requirements placed on users.

The human memory has limitations which affect the ability to recall complex passwords that must be constantly changed (Kinsbourne & George, 1974). The review of literature revealed that while using strong passwords improve security, using them and constantly changing them places too much cognitive load on users (Novakovic et al., 2009). Novakovic et al. (2009) then mentioned that the use difficult passwords have a negative impact on their usage. Sridhar (2010) also concluded that when designing information security infrastructures, the human side must be considered in a way that limits the cognitive overload by using complex passwords.

The cognitive load theory has also been studied in other are areas dealing with technology, Chilton and Gurung (2008) conducted an experimental study in which they investigated how advanced technology impacts the cognitive load and affects student learning outcomes. Cognitive load in this context was described as being dependent on two things which are the student's ability to deal with intrinsic cognitive loading and extrinsic cognitive loading (Paas & Kester, 2006). Intrinsic cognitive loading was defined to deal with the complexity of the material to be learned while extrinsic cognitive loading is a function of the presentation of the material to be learned as well as the leaning activities (Chilton & Gurung, 2008). Paas and Kester (2006) concluded that controlling in student learning, as complexity of the task increases, intrinsic load also increases and therefore controlling the cognitive load is important in achieving a meaningful and efficient learning outcomes in the instructional environment. Boechler (2006) noted that a condition known as cognitive overload occurs when available cognitive resources are surpassed and this leads to performance on memory learning tasks being degraded.

Table 4: Summary of Literature for Cognitive Load Theory

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
Boechler, 2006	Literature Review and Synthesis		Human Memory System	When available cognitive resources are surpassed, performance on memory and learning tasks is degraded, a condition referred to as cognitive overload.
Carstens et al., 2004	Empirical Study via Survey and Experiment	250 Survey Participants 30 Experiment Participants	Password Authenticatio n	A password that is too complex is difficult for users to remember.
Chilton & Gurung, 2008	Experimental Design	95	Factor Analysis	The effects of advanced technology on student learning outcomes
Crawford, 2013	Empirical Study via Survey	218	Password Survey	Controls used during the password creation process shape password strength, however, behavior controls do not produce significantly stronger passwords that

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
				informal controls.
Fan & Lei, 2008	Empirical Study via Experiment	21	Performance Algorithms	Machine intelligence is supplemental to human users and assists the users to deal with cognitive overload and make appropriate decisions for the model building process.
Henry, 2007	Empirical Study via Experiment	139	Password Usability	The input of the precise formulation of robust passwords was the greatest single cause of authentication failure.
Hogg, 2007	Literature Review		Nine-point Subjective Rating Scale	Describes cognitive load theory and what happens when working memory is overloaded.
Keith et al., 2009	Literature Review and Field Study	56	Passphrases	The use of passphrases result in cognitive overload due to memory constraints by the user

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
Novakovic et al., 2009	Online Survey	111 participants	Password Survey	Difficult passwords have an impact on their usage. A user's prior computing experience influences their intentions to act securely.
Paas & Kester, 2006	Literature Review, Meta-Analysis and Synthesis		Cognitive Load Theory	Cognitive load theory argues that the interactions between learner and information characteristics can manifest as intrinsic or extrinsic cognitive load.
Shay et al., 2010	Paper Survey	450 participants	Password Handling, composition, storage, and reuse	The use of stronger passwords causes users to struggle to comply, reuse passwords as well as to write them down.
Sridhar, 2010	Case Study	One Organization	Information Security Management	For a robust information security infrastructure, organizations must also consider the human side.
Sweller, 1988		24		Conventional problem solving

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
	Empirical Study via Experiment		Sine, Cosine, and Tangent Ratios	means-end analysis may impose a heavy cognitive load.

Productivity in Information System

According to Weihrich and Koontz (1994), productivity deals with the output-input ratio within a time period with due consideration for quality. They also claimed that productivity implies effectiveness and efficiency in individual as well as organizational performance. Organizations invest significant resources into information technology because of its ability to affect the productivity of the workers (Wierschem & Brodnax, 2003). Productivity has an effect of information systems, Natarajan, Rajah, and Manikavasagam (2011) mentioned that measuring the productivity of employees has been one of the concerns for IT organizations worldwide. Natarajan et al. (2011) defined knowledge worker productivity as the measure of the efficiency and effectiveness of the output generated by workers who mainly rely on knowledge as opposed to labor in the course of production. Natarajan et al. (2011) further mentioned that situational knowledge is obtained by knowledge workers to get things done in a dynamic environment. Knowledge about passwords falls into the category of situational knowledge. Natarajan et al. also stated productivity encompasses the people as well as the systems built around them and the fact that there are different metrics that can be used to measure productivity. Whatever the measure is used, the objective of the productivity measurement should be productivity enhancement (Nachum, 1999).

Addressing the issue of IT productivity, Hernández-López, Colomo-Palacios, García-Crespo, and Cabezas-Isla (2011) pointed out the factors that influence productivity which include: increasing store constraints, timing constraints, reliability requirements, requirements volatility, staff tools skills, staff availability, customer participation, and project duration. Yi and Im (2004) argued that productivity gains resulting from the use of IS cannot be realized unless users have the requisite computer skills. Yi and Im (2004) then concluded that a good understanding of factors that affect productivity and task performance is important as this affect the ultimate organizational success. There are usability issues with current authentication solutions when accessing the system, this has an impact of both productivity as well as task performance and therefore warrants further study.

Table 5: Summary of Literature for Productivity in Information System

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
Hernández-López, Colomo-Palacios, García-Crespo, and Cabezas-Isla, 2011	Literature Review and Synthesis		Software Engineering Productivity	There is lack of study in many different countries about productivity analysis and the gap has to be covered because software development environment and culture are different in each country.
Nachum, 1999	Literature Review and Synthesis		Productivity Measure	An inadequacy of the manufacturing-based

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				measurement procedures and demonstrate that a measure which acknowledges the unique characteristics of professional services correlates better with firms' performance exist.
Natarajan et al., 2011	Literature Review and Synthesis Case Study	One Non-profit organization	Password Survey	There is no fool proof method to enhance personnel productivity assessment methods for IT companies.
Wierschem & Brodnax, 2003	Empirical Study via Experiment	149 participants	End User Productivity	The results of this study identify that an improvement in processor speed of 47% produced a direct productivity improvement of 4.4% validating the unqualified business management’s assumptions that technological improvements do in fact enhance worker productivity are supported.

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
Yi & Im, 2004	Empirical Study via Experiment	41 students	Computer Task Performance	Personal goal was a significant predictor of computer task performance. Past experience and age were also significant predictors of computer task performance.

Role of Help Desk and End-User Support

Iwai, Iida, Akiyoshi, and Komoda (2010) stated that responding to the inquiries by users as the most fundamental task of help desk. Millhouse (2009) described the help desk as the sector used in managing an organization's IT infrastructure. Lee, Kim, and Lee (2001) conducted a survey and the results revealed that end-users rely on the telephone, e-mail, and in-person (face-to-face) as the main ways of contacting the help desk. Thomas (2009) mentioned that the help desk is the front line for various users seeking assistance when conducting business. Delic and Hoellmer (2000) pointed out that the help desk is an integral part of many organizations that must support products of services. They further claimed that analysts with varying levels of expertise occupy the help desk and their responsibilities include addressing a wide range of problems from customers or clients. As the problems come in, they are addressed at different layers within the help desk and there is a cost associated with the solution. The "rule of four" has been suggested and it basically states that the cost of treating the problem on the first contact is multiplied by four if the problem is forwarded to the next layer (Delic & Hoellmer, 2000). Lee et al. (2001) mentioned that growing demands and expectations of end users led the help desk services to look for better ways to provide user support services. Some of the ways include combining technology-enabled tools with conventional human-based support in an effort to provide an effective and efficient end user support.

Part of the responsibilities of help desk staff deals with determining whether the issue is desktop, system, or access related (Thomas, 2009). Password problems are handled by the help desk since they are access related. As the help desk gets involved in resetting passwords as well as other break fix issues, it becomes important to find ways of offering those services while minimizing technology related downtime within the organization (Wiggins, 2012).

Table 6: Summary of Literature for Role of Help Desk and End-User Support

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
Delic & Hoellmer, 2000	Case Study	One customer support center	Help Desk Support	Knowledge-based support calls were shorter that those without such support.
Iwai, Iida, Akiyoshi, & Komoda, 2010	Case Study		Help Desk Support	A help desk support system with filtering and reusing inquiries by e-mail was proposed.
Lee, Kim, & Lee, 2001	Empirical Study via Survey	214 users	Help Desk Perception	The use of in-person media is related to increase in end-

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				users' perception on service assurance.
Millhouse, 1999	Theoretical		Help Desk Analysis	There remained a core of independent help desk vendors that are generally considered to be workgroup-oriented.
Thomas, 2009	Case Study		Interactive Help Desk	Content relevant to the Administrative Systems functions within a Help Desk dashboard system are the most difficult to maintain because of continuous updates and process changes.
Wiggins, 2012	Theoretical		Help Desk Support	When implementing a new solution, it would best to take baby steps when making major changes and not to try to change everything at once.

Single-Sign-On

Single-Sign-On (SS) technology can be implemented to mitigate some of the shortcomings associated with the password authentication (Heckle, Lutters, & Gurzick, 2008). Benkhelifa, Fernando, and Welsh (2013) mentioned SSO as a process that enables a user to have single user credentials to gain access to multiple applications and resources which have been assigned to the user. However, it should be noted that while SSO improves user experience and relieves the burden of remembering several passwords, it can introduce new security challenges (Heckle et al., 2013). Benkhelifa et al. (2013) used Figure 2 to demonstrate the concept of SSO.

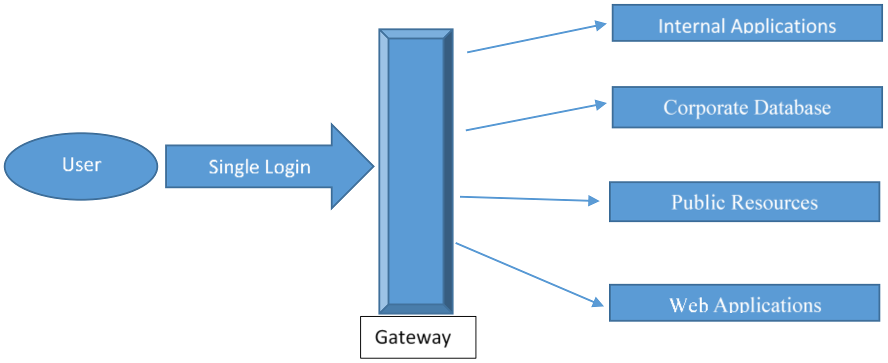


Figure 3. Single-Sign-On (Benkhelifa et al., 2013)

While SSO provides a solution of reducing the burden on user's memory, there will still be need to remember a single master password (Sun, Boshmaf, Hawkey, & Beznosov, 2010). Bauer, Bravo-Lillo, Fragkaki, and Melicher (2013) noted that SSO reduces the many sets of credentials that users have to present, however, they still need to provide a set of credentials to a service provider. Sun et al. (2010) also mentioned that SSO technology come with their challenges which include the difficulty users might experience migrating their existing passwords to the system as well as users not trusting the security of the systems. SSO solutions rely on protocols when the set of credentials are submitted are supplied to a service provider, there are vulnerabilities with authentication protocols as they are known to be prone to design errors (Gross, 2003). Organizations with legacy systems have to incur additional costs for new infrastructure in order to implement different SSO methods provided by different vendors (Tiwari & Joshi, 2009). SSO's implementation also reveals hidden complexities as trust relationships between federated parties are harder to establish especially if one party has a significantly higher risk exposure than the other (Heckle et al., 2013).

Table 7: Summary of Literature for Single-Sign-On

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
Bauer, Bravo-Lillo, Fragkaki, & Melicher, 2013	Empirical Study via Survey	482 participants	Interaction Design	Some preferences of users appear to be out of sync with current implementations of the SSO process.
Benkhelifa et al., 2013	Investigative and Comparative Study		Hybrid of SSO and MFA	The proposed hybrid SSO and two-factor authentication appears to a highly secure authentication approach.
Gross, 2003	Theoretical		SSO security analysis	The SAML Single Sign-on Browser/Artifact profile is in general a well-written protocol, nevertheless, several changes

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				are required to improve its security and prepare for its broad application in industry.
Heckle et al., 2013	Field Study	One Hospital	Discerning both the process and factors impacting both usability and security	To fully realize the intended usage of SSO, the user's mental models must also be adjusted to reflect the SSO environment, not just the SSO technology.
Sun et al., 2010	Literature Review and Comparative Analysis		Web SSO adoption	Web SSO systems pave a critical foundation for the user-centric web where users won their personal content and are free to share.
Tiwari & Joshi (2009	Investigative Study		SSO with Password	Other robust method of implementing single sign on feature are generally infeasible when the organization wants to

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				implement it in its legacy system with minimum changes.

Multi-Factor Authentication

To increase the overall security during the authentication process, the multi-factor authentication (MFA) has been suggested and it requires two or more authentication factors in order to allow access to IS resources (Benkhelifa et al., 2013). MFA requires the authentication to be based on two or more factors, Menkus (1998):

- Biometric-based authentication – what the user is
- Possession-based authentication – what the user has
- Knowledge-based authentication – what the user knows

Chaudhary, Tomar, and Rawat (2011) noted that since MFA offers the highest information security through multiple layers using multiple authentication factors, it provide less user convenience. Czeskis, Dietz, Kohno, Wallach, and Balfanz (2012) shared the same sentiments when they mentioned that MFA have the potential of increased security but at the expense of usability, deployability challenges as well as failing to provide sufficient protection against phishing attacks. Wang, He, Wang, and Chu (2014) mentioned that the most common type of convenient and effective type of MFA is the password authentication and smart card authentication, however, despite decades of research, it remains a challenge to design a practical and anonymous MFA scheme. Wang et al. (2014) further noted that even though the password authentication with smart card has been deployed in various kinds of applications, the main challenges are privacy and usability. Gunson, Marshall, McInnes, Morton, and Jack (2014) conducted a study in which subjects used two factors of authentication which were voice and a secret number, users indicated that the process was longer than usual in their evaluation for the authentication process. Figure 3 below illustrates the MFA concept.

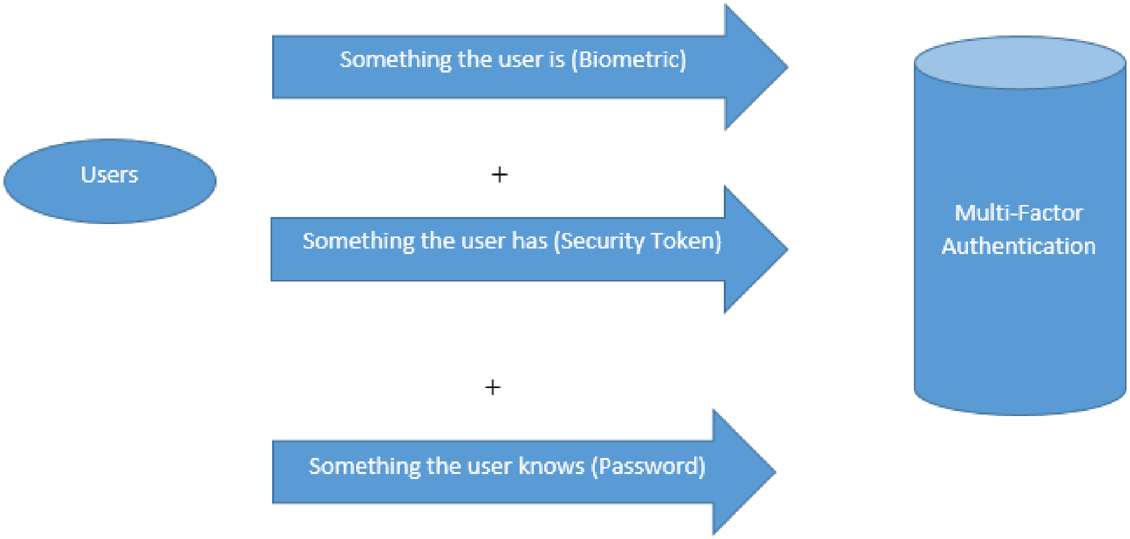

Something the user is (Biometric)
Users
+
Something the user has (Security Token)
+
Something the user knows (Password)
Multi-Factor Authentication

Figure 4. MFA (Chaudhary et al., 2011)

On how MFA can be implemented, Chaudhary et al. (2011) further suggested implementing policies that consider the category of the user group and then basing the method of authentication on the group that users belong to. The first group identified was the Intranet users group with users who access the network resources from within the organizational boundaries, pass through well-defined physical authorization and authentication mechanisms which make them part of a trusted user group. Chaudhary et al. (2011) concluded this group can use the single factor authentication method like the conventional userID/Password. The second group consists of Extranet users who access the networked resources from outside the organizational boundaries, however, they use well defined logical authorization and authentication mechanisms. This would be classified as a partially trusted group. The third group would be Internet users who access networked resources from outside the organizational boundaries using public networks without passing through any formal identity test, this group would be the least trusted user group. Chaudhary et al. (2011) further concluded that Internet users require the most complex authentication like the MFA to ensure highest security. The three categories of authentication that can be used in MFA are Something the User Is (Biometrics), Something the User Has (Security Token or Smart Card), and Something the User Knows (Passwords).

Password + Smart Card

Yu, Wang, Mu, and Gao (2014) pointed out that a system which authenticates users by using a password and a smart card can be referred to as a two-factor authentication. An example when two-factor authentication is used is in banking when a client can pass authentication only if the client provides a correct password and a corresponding smart card. While just the password authentication mechanism remains the popular authentication methods, it has proven to have some limitations leading to attacks such as dictionary attacks. One of the solutions suggested to such limitations is using smart cards along with the password resulting in two factor authentication which can lead to higher security guarantees (Yu, Wang, Mu, & Gao, 2014).

Password + Biometric

In an effort to provide an overall solution to secure information access and improve the limitations that the password authentication method has, Ngugi, Tarasewich, and Recce (2012) pointed out that the solution will have to include a number of measures and countermeasures. As a solution, Ngugi et al. (2012) suggested adding an additional biometric layer to the current authentication systems by making use of a keypad which used timing patterns to verify that the person typing the password is the actual owner of the account. Chudá and Ďurfina (2009) proposed an authentication method which uses both the password and biometric to provide access to the system. The password would be text-based while the biometric would be the keystroke demonic. The keystroke dynamic, based on user behavior typing text on the keyboard uses the rhythm and the way user's type then stores the dynamics for the purpose of making a unique biometric template of the user typing for the future authentication. Chudá and Ďurfina (2009) concluded that the password and keystroke dynamic combination can be used in situations without high security demands and not in high security systems such as those involving financial transactions.

Password + Smart Card + Biometric

The use of a password along with a smart card is considered to be secure as compared to simply using one method, however, it can also present some challenges in the event that a password is small, forgotten or lost and a smart card is stolen (Yu, Wang, Mu, & Gao, 2014). Adding the biometric to a password and smart card authentication scheme can potentially increase security and this will result in a three factor authentication.

Table 8: Summary of Literature for Multi-Factor Authentication

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
Benkhelifa et al., 2013	Investigative and Comparative Study		Hybrid of SSO and MFA	The proposed hybrid SSO and two-factor authentication appears to a highly secure authentication approach.
Chaudhary et al., 2011	Theoretical		Multi-layer MFA with Open Source	Multi-layer mechanism combined with multifactor authentication using Open Source solutions seem to provide better tradeoff between security and user convenience in varying trust networks.
Choi et al., 2014	Practical Evaluation		Biometric Scheme Analysis	Adding secret information to the registration, login and authentication phases may help a biometric scheme to overcome security problems.
Crawford, 2013	Empirical Study via Survey	218	Password Survey	Controls used during the password creation

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				process shape password strength, however, behavior controls do not produce significantly stronger passwords that informal controls.
Czeskis, Dietz, Kohno, Wallach, & Balfanz, 2012	Theoretical		Second factor authentication	An authentication scheme which uses oportunistic identity, an assertions which allow the server to treat logins differently based on how the user was authenticated – allowing the server to provide tiered access or restrict dangerous functionality was proposed.
Gunson, Marshall, McInnes, Morton, & Jack, 2014	Empirical Study via Experiment	120 participants	Voiceprint authentication	The metric on which the 2-Factor strategy scored less favorably than the Challenge

Study	**Methodology**	**Sample**	**Instruments/ Constructs**	**Main findings or contributions**
				version was the time taken to complete authentication process.
Herley- et al., 2009	Literature Review and Synthesis		Password Authentication	In the absence of tools to measure the economic losses and the effectiveness of new technological proposals, it is expected the adoption of password alternatives will continue to be difficult to justify.
Hussain & Alnabhan, 2014	Experimental Evaluation	10 participants	User login attempts	The authentication model appears to solve the problem of large deviations in keystroke dynamics and provides improved keystroke authentication level.
Hussein & Nordin, 2014	Case Study	20 participants	Password Survey	The accuracy of a palmprint recognition system depend on many

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				factors such as the acquisition of images, resolution of images, and the size of the database of the system.
Kim, 2012	Empirical Study via Questionnaire	70 participants	Password Questionnaire	A keypad which increases the time required for brute force attacks by the finder through formation of random buttons, random button arrangement and display delay time was suggested for smartphones.
Lehtonen, Michahelles, & Fleisch, 2007	Literature Review and Synthesis		RFID-Based Authentication	The level of security of any RFID-based product authentication application is determined by how it fulfills the derived set of functional and nonfunctional requirements.

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
Ma & Feng, 2011	Empirical Study via Experiment	26	Password Usability	Graphical passwords took longer time than the text password and mnemonic password. The text passwords and graphical passwords are equally memorable.
Medlin, 2013	Empirical Study via Survey	118	Password Survey	It is important for users to stay vigilant in protecting the information within a network and not just rely on computerized systems.
Menkus, 1998	Literature Review		Password Use	A problem exists with various password schemes and that is they offer limited password security.
Ngugi & Kamis, 2013	Empirical Study via Survey	279 participants	Biometric Survey	There is need for security managers to alert biometric engineers to minimize the two factors that

Study	Methodology	Sample	Instruments/ Constructs	Main findings or contributions
				degrade system response efficacy of a biometric system.
Wang, He, Wang, & Chu, 2014	Case Study		Password and Smart Card	It is difficulty to build an anonymous two factor authentication scheme due to usability-security tradeoffs.

Summary of What is Known and Unknown in the Research Literature

This literature review provides a theoretical foundation for this study as it has demonstrated the factors surrounding the authentication method of passwords. Results of prior research studies demonstrated that passwords are the widely used method of authentication for computers, networks, and Websites among other systems (Kim, 2012). Researchers agree that password security is important and security policies can be put in place to improve password security (Inglesant et al., 2012). Shay et al. (2010) noted that while strong password polices improve information security, it creates a challenge that those users may have a difficult time remembering the passwords. Carstens et al. (2004) pointed out the need to improve security as well as investigating the balance between complexity and productivity. Novakovic et al. (2009) further claimed that using strong passwords and constantly changing them can have counterproductive effects as it places too much cognitive load on the users. However, their study did not actually manipulate or change the strength of the passwords as they measured responses from users on a 5 point Likert scale. Herley (2009) agreed with the claim above and also stated that too complex passwords may create a situation in which users forget their passwords thereby having a negative effect on production and task completion. Crawford (2013) conducted a research study to investigate the password creation process and mentioned that individuals are required to maintain large numbers of passwords and that can lead to cognitive overload. Several studies have been conducted to confirm that strong and complex passwords cause cognitive overload, however, the point at which the overload occurs has not been investigated. As such, this study research is aimed at investigating the point at which the increase of the cognitive load becomes counterproductive.

Productivity has an effect of information systems, Natarajan, Rajah and Manikavasagam (2011) mentioned that measuring the productivity of employees has been one of the concerns for IT organizations worldwide. Addressing the issue of IT productivity, Hernández-López, Colomo-Palacios, García-Crespo, and Cabezas-Isla (2011) pointed out several factors that influence productivity.

Iwai, Iida, Akiyoshi, and Komoda (2010) stated that responding to the inquiries by users as the most fundamental task of help desk. Lee, Kim, and Lee (2001) conducted a survey and the results revealed that end-users rely on the telephone, e-mail, and in-person (face-to-face) as the main ways of contacting the help desk.

The single-sign-on technology is a ways which has been implemented to mitigate the shortcomings associated with password authentication (Heckle, Lutters, and Gurzick, 2008). The single-sign-on technology is a process that enables a user to have single user credentials to gain access to multiple applications and resources which have been assigned to the user (Benkhelifa, Fernando, & Welsh, 2013) Sun et al. (2010) also mentioned that SSO technology come with their challenges which include the difficulty users might experience migrating their existing passwords to the system as well as users not trusting the security of the systems. SSO solutions rely on protocols when the set of credentials are submitted are supplied to a service provider, there are vulnerabilities with authentication protocols as they are known to be prone to design errors (Gross, 2003). Organizations with legacy systems have to incur additional costs for new infrastructure in order to implement different SSO methods provided by different vendors (Tiwari & Joshi, 2009).

The multi-factor authentication has been introduced to increase the overall security during the authentication process and it requires two or more authentication factors in order to allow access to IS resources (Benkhelifa et al., 2013). Chaudhary, Tomar, and Rawat (2011) noted that since MFA offers the highest information security through multiple layers using multiple authentication factors, it provide less user convenience. Czeskis, Dietz, Kohno, Wallach, and Balfanz (2012) shared the same sentiments when they mentioned that MFA have the potential of increased security but at the expense of usability, deployability challenges as well as failing to provide sufficient protection against phishing attacks. Wang et al. (2014) noted that even though the password authentication with smart card has been deployed in various kinds of applications, the main challenges are privacy and usability.

Chapter 3

Methodology

Research Design

To investigate the effect of changing the cognitive load (via different password strengths), a lab experiment was proposed and conducted. Three groups were used; two experimental groups and one control group (Ellis & Levy, 2011). Two experimental groups (Group A & Group B) were constructed with 24 users in each group. A third group (Group C) was constructed as the control group, and also had 24 users. The study participants in the three groups came from a local college in different majors at different levels in their academic levels. The degree programs offered by the college include Accounting, Automotive Technology, Business Management, Computers and Digital Media, Graphic Arts, Construction Management, as well as Nursing. Students enrolled in the above degree programs comprise of traditional students who just graduated from high school, adult learners seeking to further their education as well as dislocated workers. All users in the three groups were randomly assigned. The experiment was conducted over a period of 11 weeks.

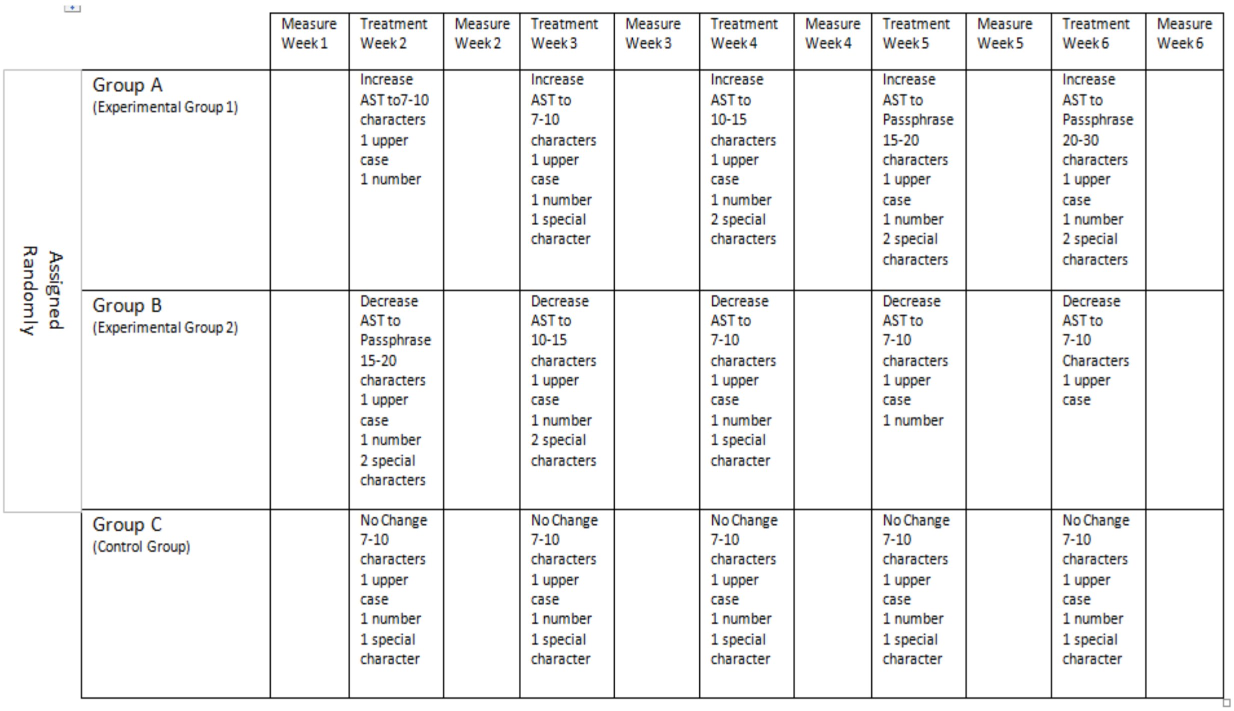
The users had different password strengths required based on the group membership and time within the experiment. The first experimental group (Group A) began with a password that was at least seven characters long and with at least one uppercase letter in week one. Inglesant et al. (2012) suggested that a strong password has a length of 7-8 characters, the beginning authentication strength level for the password was within the suggested strength level. Medlin and Cazier (2007) listed some of the characteristics of a strong password to include uppercase characters, lowercase characters, and numbers, all those factors were included in the initial password. As listed in Figure 1, the authentication strength level was increased in week two through week six, and their performance was measured during each week based on:

- Average number of failed OS logon attempts
- Average logon times
- Average task completion
- Number of requests for assistance (unlock and reset account)

The authentication strength level was the strongest in week six, when it increased to include a passphrase with 20-30 characters, one uppercase letter, one number, and two special characters. After the performance was measured, the authentication strength began to decrease in weeks seven through week 11 and the performance was measured in each of those weeks as well.

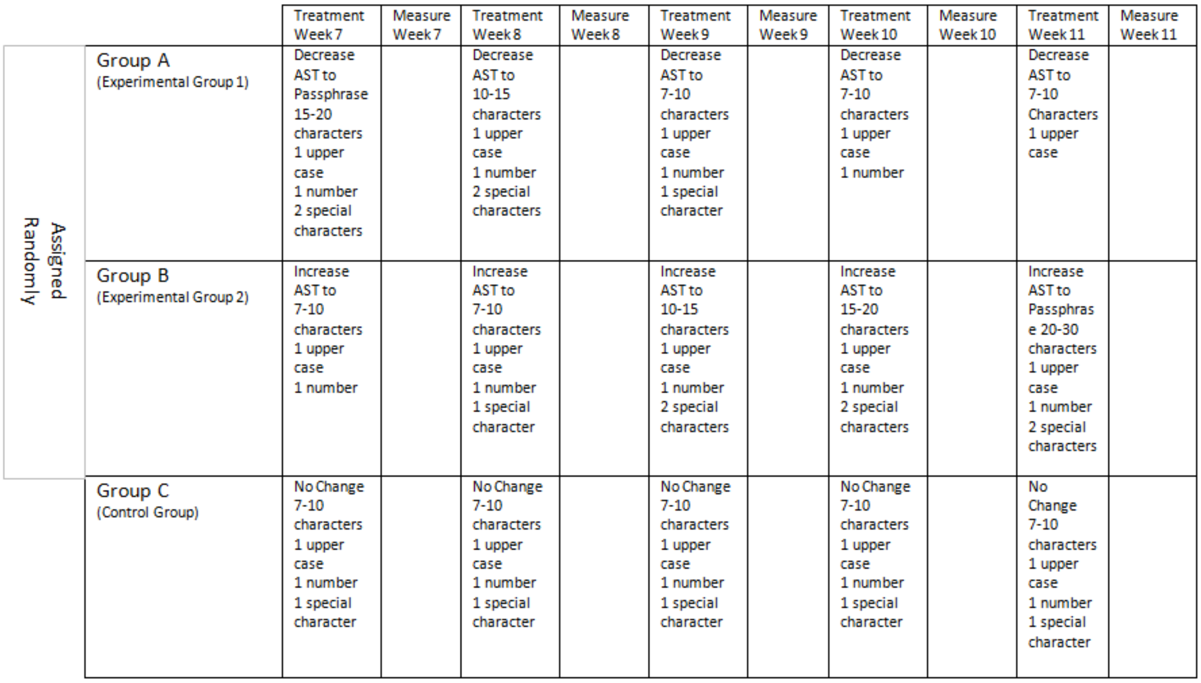
The second experimental group (Group B) began in week one with a password that included a passphrase with 20-30 characters, one uppercase letter, one number, and two special characters. As listed in Table 2a, it decreased each week until week six when it was 7-10 characters with one uppercase letter. The performance for Group B was measured during each week based on the same criteria that was used for Group A. As listed in Figure 1, the password strength for Group B began to increase in week seven through week 11 and the performance was measured each week as well. Figure 1 illustrates how the password strength was manipulated throughout the experiment.

Table 9a: Experimental Design – Authentication Strength (AST) – Week One to Week Six



		Measure Week 1	Treatment Week 2	Measure Week 2	Treatment Week 3	Measure Week 3	Treatment Week 4	Measure Week 4	Treatment Week 5	Measure Week 5	Treatment Week 6	Measure Week 6
Assigned Randomly	Group A (Experimental Group 1)		Increase AST to7-10 characters 1 upper case 1 number		Increase AST to 7-10 characters 1 upper case 1 number 1 special character		Increase AST to 10-15 characters 1 upper case 1 number 2 special characters		Increase AST to Passphrase 15-20 characters 1 upper case 1 number 2 special characters		Increase AST to Passphrase 20-30 characters 1 upper case 1 number 2 special characters	
	Group B (Experimental Group 2)		Decrease AST to Passphrase 15-20 characters 1 upper case 1 number 2 special characters		Decrease AST to 10-15 characters 1 upper case 1 number 2 special characters		Decrease AST to 7-10 characters 1 upper case 1 number 1 special character		Decrease AST to 7-10 characters 1 upper case 1 number		Decrease AST to 7-10 Characters 1 upper case	
	Group C (Control Group)		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character	

Table 9b: Experimental Design – Authentication Strength (AST) – Week Seven to Week 11



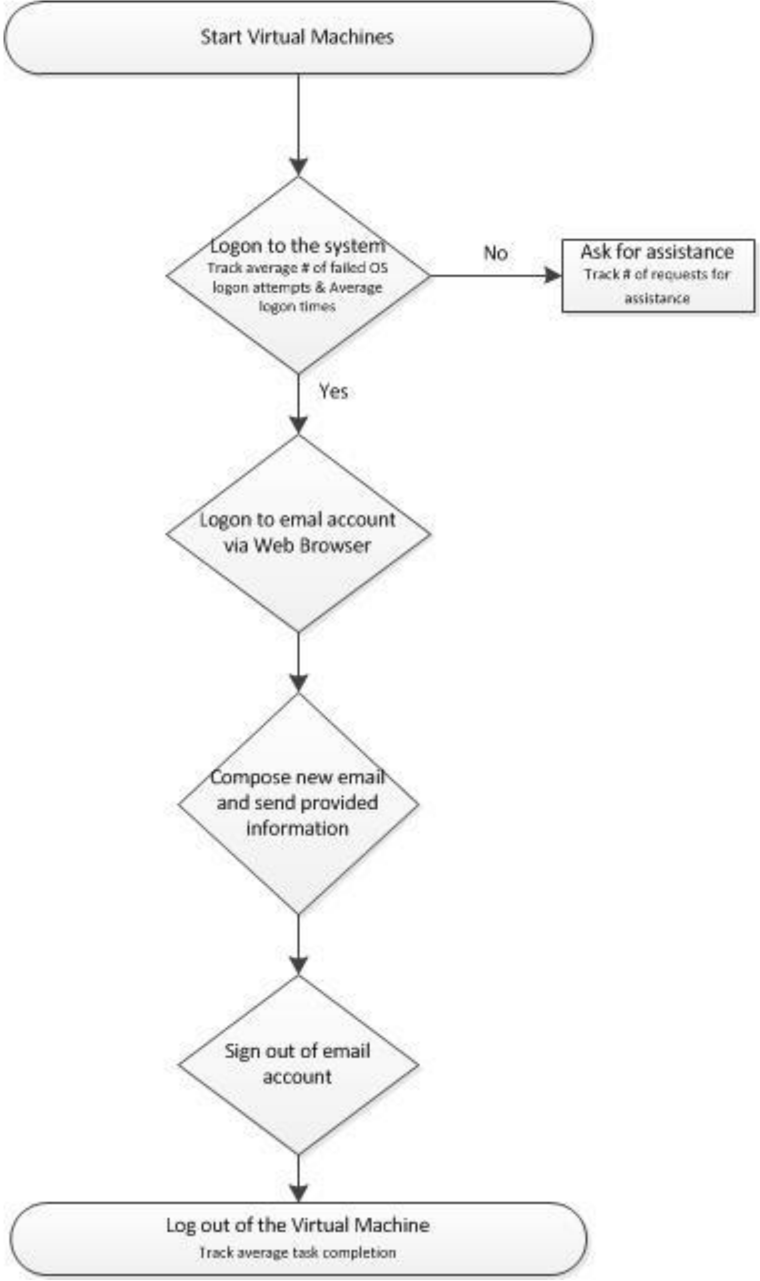
		Treatment Week 7	Measure Week 7	Treatment Week 8	Measure Week 8	Treatment Week 9	Measure Week 9	Treatment Week 10	Measure Week 10	Treatment Week 11	Measure Week 11
Assigned Randomly	Group A (Experimental Group 1)	Decrease AST to Passphrase 15-20 characters 1 upper case 1 number 2 special characters		Decrease AST to 10-15 characters 1 upper case 1 number 2 special characters		Decrease AST to 7-10 characters 1 upper case 1 number 1 special character		Decrease AST to 7-10 characters 1 upper case 1 number		Decrease AST to 7-10 Characters 1 upper case	
	Group B (Experimental Group 2)	Increase AST to 7-10 characters 1 upper case 1 number		Increase AST to 7-10 characters 1 upper case 1 number 1 special character		Increase AST to 10-15 characters 1 upper case 1 number 2 special characters		Increase AST to 15-20 characters 1 upper case 1 number 2 special characters		Increase AST to Passphrase 20-30 characters 1 upper case 1 number 2 special characters	
	Group C (Control Group)	No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character	

The control group (Group C) had the same authentication strength level in the password throughout the 11 weeks. The password was at least 7-10 characters, one uppercase letter, one number, and one special character. The performance for Group C was measured each week based on the same criteria used for Group A and Group B.

Experimental Activities

To test the effects of changing the cognitive load (via different password strength), a system was set up and all three groups were asked to logon to the system. Once the users were logged on, they were asked to perform specific tasks. The tasks which were performed were to logon to their email addresses from the Web, compose a new email, and send it with provided information to an email address which was provided. Table 10 below outlines the tasks that were performed.

Table 10: Experiment Flow Chart


Start Virtual Machines
Logon to the system
Track average # of failed OS logon attempts & Average logon times
No
Ask for assistance
Track # of requests for assistance
Yes
Logon to emal account via Web Browser
Compose new email and send provided information
Sign out of email account
Log out of the Virtual Machine
Track average task completion

The system tracked the average number of logon attempts for all the three groups. It also tracked the average time it took for each user to logon to the system, as well as the average time they took to complete specified tasks to emulate workplace tasks. The system had auditing mechanisms built in to track and measure all the tasks above. For the users who requested assistance with resetting passwords, the number of times the password was reset over the period of the experiment was also tracked. Users were not allowed to write passwords down, use notebooks or any other electronic devices during the experiment.

Experimental Research Measures

This study had four dependent variables (DV) and they are listed below.

a. DV1 - number of failed OS logon attempts (NFOLA)

b. DV2: - average logon times (ALT)

c. DV3: - average task completion times (ATCT)

d. DV4: - number of requests for assistance (unlock and reset account) (ARA)

The measures for ALT and ATCT were continuous; while NFOLA and ARA were ordinal. The first dependent variable, NFOLA, was automatically collected by Server 2008 as the users attempted to logon to the system. As the users entered a wrong password, the system recorded the entry and the reports from the log files were collected every week. The second and third DVs, were also recorded by the system and the results were collected from the Windows log files. The auditing logs were used to record ATCT by looking at the time users started the logon session until the time they log off. The last DV, ARA, was measured each time a user requested their password to be reset. The Account Lockout Threshold in Server 2008's Group Policy Management Editor was set to three and when that threshold was reached users had to seek assistance. The data was recorded for all the four DVs.

The independent variable (IV), cognitive load (via different password strengths) listed in Tables 9a and 9b was administered to all the groups over the 11-week period of the experiment. Carstens et al. (2004) mentioned that using complex passwords places a cognitive overload on the users, the cognitive load was raised as the week progress for Group A, decreased for Group B, stay the same for Group C. The use of passphrases which consist of several words have been suggested as affecting the cognitive load of users and the length of the password was manipulated each week (Keith et al., 2009). Passwords which are too long to be managed in short memory may be too difficult for users to memorize which can possibly lead to users writing the passwords down (Keith et al., 2009). There were three control variables (CV) in this study and they were age, gender, and computer experience. Sekeran (2003) pointed out that demographic information helps to describe the information of a sample as well as the general population. McCloskey and Leppel (2010) mentioned that age has an impact on how users participate in electronic activities. Awwal (2012) pointed the need to measure specific consumer groups following a research which showed different study results based on age and gender. The need to measure based on gender was validated by Banerjee, Kang, Bagchi-Sen, and Rao (2005), they concluded that there are different behaviors among males and females when using Internet services. The performance measures in this study were also controlled for computer use experience. Hoxmeier, Nie, and Purvis (2000) listed experience with electronic communications as one of the most important direct factor that affect user confidence and effectiveness when performing computing operations. The CVs were collected at the beginning of the experiment. Each week, information about the DVs were collected when controlled for the CVs.

Validity and Reliability

Trochim and Donnelly (2008) defined validity as the best available approximation to the truth of a given proposition, inference, or conclusion and reliability as repeatability and consistency. In this study, the pretest-posttest with control group design was used because of its strength in controlling threats to internal validity (Campbell & Stanley, 1963). Types of validity include internal, external, and construct (Straub, 1989; Trochim & Donnelly, 2008).

Straub (1989) mentioned internal validity as one that asks the question whether observed effects or results could have been caused by unmeasured variables. Campbell and Stanley (1963) defined internal validity as “the basic minimum without which any experiment is uninterpretable: Did in fact the experimental treatments make a difference in this experimental instance?” (p. 5). There were several threats to internal validity that were addressed in this study. The first one had to deal with users selecting the option of saving their passwords or writing them down. Measures were put in place to ensure students did not have the ability to save passwords or write them down. The use of notebooks or any electronic devices was prohibited during the experiment. For the average logon times and average task completion times variables, a program called Vision was used to block access to desktops before tasks were given so that students began at the same time. Interruptions during task could also affect the results and, therefore, measures were put in place to control every interruption. The network was fully tested to ensure the Active Directory authentication server was available during the experiment time.

External validity deals with how the results can be generalized to other settings or population (Sekeran, 2003). Simply put, external validity “asks the question of generalizability: to what populations, settings, treatment variables, and measurement variables can this effect be generalized?” (Campbell & Stanley, 1963, p. 5). The study participants in this experimental study came from different majors as well as different levels academically which is important in ensuring the results have implications for other groups and individuals in other settings as well as at other times (Staub, 1989). The tasks which the users performed during the experiment were login to a computer, signing into an email account, composing an email message, sending the email with given data, signing out of the email account and then login off the computer. The tasks were selected as they provide results which are similar to the tasks that are performed by computer end users in real-world operational environments. The tasks represented daily tasks which are performed in the computer environment by experts in different fields like medicine and geology (Costabile, Fogli, & Lanzilotti, 2006). The fact that the sample size in this study was homogeneous was important as it provided additional validity for the measured effect of the treatment (Levy & Ellis, 2011).

The construct validity addresses the question as to whether the study or program implemented what it intended to implement and whether the intended measure was the one measured (Trochim & Donnelly, 2008). This study attempted to measure the point at which the increase of the cognitive load (via different password strength) becomes counterproductive to an organization and results collected from NFOLA, ALT, ATCT, and ARA will provide that information.

Proposed Sample

Students in three sections of the Computer Concepts and Applications class at a medium-sized two-year college in the Midwestern United States were used as the sample in this study. Students enrolled in all the degree programs offered by the college take the Computer Concepts and Application class. The degree programs offered by the college include Accounting, Automotive Technology, Business Management, Computers and Digital Media, Graphic Arts, Construction Management, and Nursing. Students enrolled in the above degree programs comprise of traditional students who just graduated from high school, adult learners seeking to further their education as well as dislocated workers. This sample was selected because of its generalizability, which is the degree to which study conclusions are valid for members of the population not included in the study sample (Trochim & Donnelly, 2008). The course is a requirement for every student at the college. Students in this class represent different majors offered at the college. Some students decide to take the class at the beginning of their academic journey while others take it in the final semester. The maximum number of students in each of the course was 24. Lutu (2005) confirmed that a sample size is considered statistically valid if it has a true representation of the database from which it was selected.

Pre-analysis Data Screening

Levy (2006) mentioned that pre-analysis and data screening is important as it ensures that the data to be analyzed is accurate and reliable. Mertler and Vannatta (2010) highlighted the following four reasons for pre-analysis and data screening: a) the accuracy of the data collected, b) missing data and attempts to assess the effect of and ways to deal with incomplete data, c) assess the effect of extreme values, d) assess the adequacy of fit between the data and the assumptions of a specific procedure. Data was collected each week during the experiment, which includes NFOLA, ALT, ATCT, and ARA. In the event of missing data, the first alternative was to estimate missing values and the second alternative was to drop the variables. The statistical procedure Mahalanobis distance was used to identify any multivariate outliers in the data. The Mahalanobis distance is a statistical procedure used to identify outliers of any type, it is the distance of a case from the centroid of the remaining cases and the centroid is the point created by means of all variables (Mertler & Vannatta, 2010). When multivariate outliers were identified, they were investigated further in an effort to determine whether they were due to an error in data entry, an instrumentation error or the subject being simply different from the rest of the sample (Mertler & Vannatta, 2010). Errors in data entry result in the data value being corrected while the other errors result in removing the case from the analysis.

Data Analysis

Mertler and Vannatta (2010) noted the multivariate analysis of covariance (MANCOVA) as a test that investigates group differences when there is one independent variable affecting two or more dependent variables. The MANOVA test was used to assess group differences for the four variables of NFOLA, ALT, ATCT, and ARA, therefore, hypotheses H1, H2, H3, and H4 were analyzed using MANOVA. The MANCOVA test was used to analyze the hypotheses H1a, H1b, H1c, H2a, H2b, H2c, H3a, H3b, H3c, H4a, H4b, and H4c in an effort to determine if a causal relationship exist between cognitive load (via different password strengths) and NFOLA, ALT, ATCT, and ARA while adjusting for covariates. The main difference between the multivariate analysis of variance MANOVA and MANCOVA is that the latter allows for adjusting with one or more covariates (Mertler & Vannatta, 2010). MANCOVA appears to fit well for this study as the increase of the cognitive load was controlled for age, gender, and computer experience. The fact that there were covariates warranted using both MANCOVA and MANOVA.

The analysis of data collected and reflected was helpful in determining the point at which the cognitive load (via different password strength) becomes counterproductive to the organization. Table 10 shows a summary of the null hypothesis analysis which were either accepted or rejected based on the results.

Table 11. Summary of Null Hypothesis Analysis

	Hypothesis Analysis	
H1	There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).	The MANOVA test will be used to check for statistical differences between group A, B, and C.
H1a	There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.	MANCOVA test will be used to compare the effects of computer experience on NFOLA between the groups. The data will be analyzed using the SPSS statistical software.
H1b	There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.	MANCOVA test will be used to compare the effects of age on NFOLA between the groups. The data will be analyzed using the SPSS statistical software.
H1c	There will be no significant differences on the number of failed OS logon attempts between the	MANCOVA test will be used to compare the

	increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.	effects of gender on NFOLA between the groups. The data will be analyzed using the SPSS statistical software.
H2	There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).	The MANOVA test will be used to check for statistical differences between group A, B, and C
H2a	There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.	MANCOVA test will be used to compare the effects of computer experience on ALT between the groups. The data will be analyzed using the SPSS statistical software.
H2b	There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.	MANCOVA test will be used to compare the effects of age on ALT between the groups. The data will also be analyzed using the SPSS statistical software.
H2c	There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.	MANCOVA test will be used to compare the effects of gender on ALT between the groups. The data will be analyzed using the SPSS statistical software.
H3	There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).	The MANOVA test will be used to check for statistical differences between group A, B, and C.

H3a	There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.	MANCOVA test will be used to compare the effects of computer experience on ATCT between the groups. The data will be analyzed using the SPSS statistical software.
H3b	There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.	MANCOVA test will be used to compare the effects of age on ATCT between the groups. The data will be analyzed using the SPSS statistical software.
H3c	There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.	MANCOVA test will be used to compare the effects of gender on ATCT between the groups. The data will be analyzed using the SPSS statistical software.
H4	There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).	MANOVA test will be used to compare the effects of computer experience on ARA between the groups. The data will also be analyzed using the SPSS statistical software.
H4a	There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.	MANCOVA test will be used to compare the effects of computer experience on ARA between the groups. The data will also be analyzed using the SPSS statistical software.

H4b	There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.	MANCOVA test will be used to compare the effects of age on ARA between the groups. The data will also be analyzed using the SPSS statistical software.
H4c	There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.	MANCOVA test will be used to compare the effects of gender on ARA between the groups. The data will also be analyzed using the SPSS statistical software.

Milestones

The experiment was conducted during a 16-week semester. Prior to the experiment, there were meetings held with the Computer Information Systems Department Chair to discuss the scheduling of classes for the 16-week semesters. Permission to conduct the experiment was granted by Dr. Tony Miksa, Vice President of Academic and Student Affairs and he oversees the IRB process at McHenry County College. The virtual network was setup during the first two weeks of the selected semester. The first two weeks of the selected semester were used to show students how they start and access their Windows 7/8 virtual workstations. The experiment began the third week of the selected semester. Data analysis began soon after the eleven weeks of the experiment.

Resources

One of the main resources needed to carry out the above experiment was a computer lab with a server computer running Windows Server 2008 or Windows Server

2012 as well as workstations with Windows 7 or Windows 8. The network was setup virtually using Oracle VM VirtualBox. Licenses for the server and workstations were obtained from Dreamspark and Oracle VM VirtualBox is free. The computer lab at McHenry County College was used to setup the virtual network and permission was granted. SPSS software was used for statistical analysis. Three classes with at least 24 enrolled students were another requirement for the study.

Summary

This chapter provided an overview of the methodology that was utilized to conduct this study. The proposed sample is described as students in three sections of the Computer Concepts and Applications class at a medium-sized two-year college in the Midwestern United States. This sample was selected because of its generalizability, which is the degree to which study conclusions are valid for members of the population not included in the study sample (Trochim & Donnelly, 2008). This chapter described the study that investigated the effect of changing the cognitive load (via different password strengths), a lab experiment is proposed. The study targeted three classes with 24 students in each class. Data was collected each week during the experiment, which includes NFOLA, ALT, ATCT, and ARA. In the event of missing data, the first alternative was to estimate missing values and the second alternative was to drop the variables. The MANCOVA test was used to analyze the hypotheses H1a, H1b, H1c, H2a, H2b, H2c, H3a, H3b, H3c, H4a, H4b, and H4c in an effort to determine if a causal relationship exist between cognitive load (via different password strengths) and NFOLA, ALT, ATCT, as well as ARA.

Chapter 4

Results

Overview

This chapter presents the results of the study analyses. A pre-analysis data screening is presented at the beginning. The results from the pretest-posttest experiment surveys are also presented. This is followed by the demographic analysis, quasi-experiment pre-analysis, and an analysis of the results from data collected during the experiment. An analysis of the tools to collect the data and the method of statistical analysis of the data are included. The chapter concludes with a summary of this study's results.

Pretest-Posttest Experiment Survey

The participants for the pretest-posttest experiment survey were selected from three Computer Concepts and Applications classes at a small community college in the U.S. As mentioned in Chapter 3, these students were selected because they represent computer users from various fields in the workplace.

Pre-Analysis Data Screening

For the pretest-posttest experiment survey, 75 users in three Computer Concepts and Applications classes were approached. 72 users consented to participate in the experiment and were, therefore, given the pretest-posttest experiment surveys after they completed the consent forms. The pretest-posttest experiment survey required users to answer eight questions about their perceptions on passwords using the instrument in Appendix A and B. The surveys were on a Likert scale, ranged from 1 being ‘Strongly Disagree’ to 7, which was ‘Strongly Agree’. Before the data analysis process could begin, a pre-analysis data screening was done. Levy (2006) has identified some reasons for the pre-analysis data screening to take place. The process of pre-analysis data screening was helpful in increasing the validity of the results as well as the accuracy of the data being analyzed. A visual inspection on the data was conducted to make sure that there was no missing data.

Finally, the Mahalanobis distance analysis was carried out on the data to identify any multivariate outliers. Table 12 and Figure 5 depict one case (UserID 1) that was identified as a multivariate outlier. UserID 1 was removed from the data set, and after the removal, 71 cases remained to be utilized for further analysis.

Table 12. Mahalanobis Distance Analysis Results

			UserID	**Value**
Mahalanobis Distance	Highest	1	1	336.16663
		2	10	40.12825
		3	11	40.12825
		4	5	35.48704
		5	16	35.48704
	Lowest	1	24	.28573
		2	23	.28573
		3	22	.28573
		4	21	.28573
		5	20	.28573a

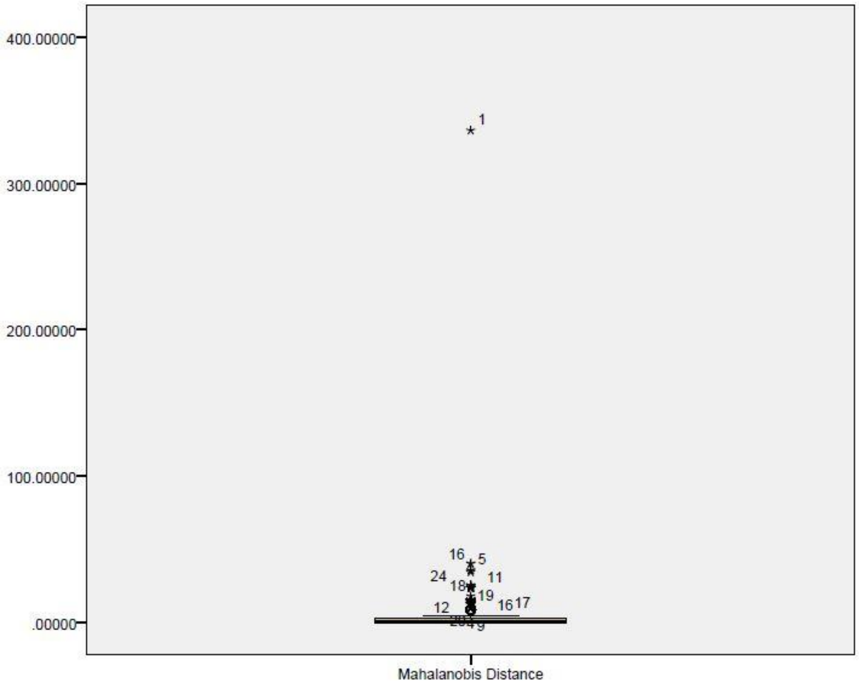


Figure 5. Mahalanobis Distance Results

Pretest-Posttest Experiment Survey Data Analysis

The MANOVA was conducted on the data collected from the pretest-posttest experiment surveys. This test was utilized to see if there were any differences in the users' perceptions about passwords before the quasi-experiment as well as after the quasi-experiment. The results from the MANOVA test indicated that there is a statistical difference between the user's perceptions about passwords before the quasi-experiment and after the quasi experiment (F = 1.210, p = 0.029) among the groups. Tables 14a and b show the mean (M) all the eight questions given to students during the pretest surveys and the posttest surveys.

Table 14a. Pretest Mean and Posttest Mean for Survey Questions by Group

	PW1	**PW2**	**PW3**	**PW4**

Group	Pre M	Post M	Pre M	Post M	Pre M	Post M	Pre M	Post M
A	5.83	5.88	6.04	5.83	6.13	5.96	6.21	5.75
B	4.67	5.96	5.33	5.96	4.83	5.86	4.63	5.92
C	5.88	6.17	5.75	5.96	6.16	6.10	5.29	5.54

Table 14b. Pretest Mean and Posttest Mean for Survey Questions by Group

	PW5		**PW6**		**PW7**		**PW8**	
Group	**Pre M**	**Post M**	**Pre M**	**Post M**	**Pre M**	**Post M**	**Pre M**	**Post M**
A	5.04	5.92	4.92	4.33	5.17	4.17	5.13	4.79
B	5.71	5.38	3.50	4.92	4.50	5.38	3.75	4.38
C	5.67	6.04	4.25	5.25	5.29	4.65	4.54	4.00

Table 15a and b show the standard deviation (SD) results for both the pretest and posttest questions.

Table 15a. Pretest SD and Posttest SD for Survey Questions by Group

	PW1		**PW2**		**PW3**		**PW4**	
Group	**Pre SD**	**Post SD**	**Pre SD**	**Post SD**	**Pre SD**	**Post SD**	**Pre SD**	**Post SD**
A	1	1.6	1.08	1.6	1.22	1.9	1.22	5.75
B	2	1.33	1.83	1.33	1.9	1.33	4.63	1.9
C	1.62	1.05	1.72	1.16	1.33	1.27	2.16	1.56

Table 15b. Pretest SD and Posttest SD for Survey Questions by Group

	PW5		**PW6**		**PW7**		**PW8**	
Group	**Pre SD**	**Post SD**	**Pre SD**	**Post SD**	**Pre SD**	**Post SD**	**Pre SD**	**Post SD**
A	1.9	1.1	1.72	2	1.52	2.2	1.62	2.38
B	1.73	1.76	1.96	1.83	2.23	1.79	2.23	1.79
C	1.43	1.04	1.85	1.57	2.02	1.65	1.93	2.02

Figures 6a, b, and c show the both the mean and standard deviation (SD) results for both the pretest and posttest questions.

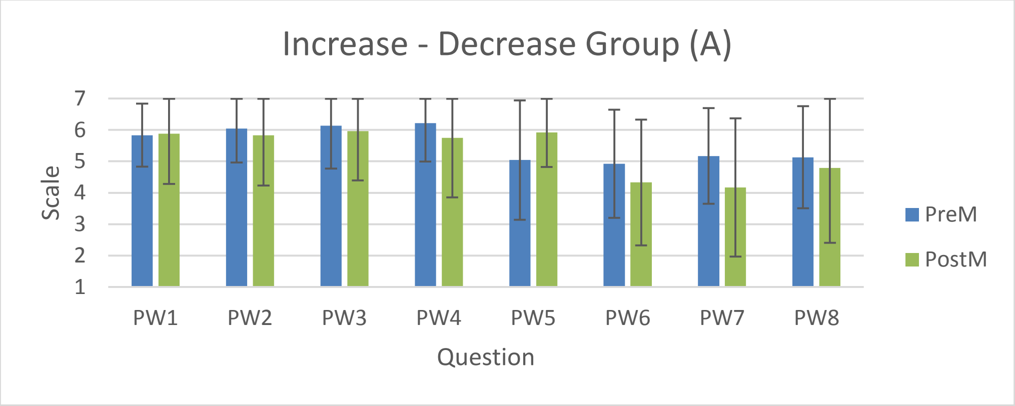


Figure 6a. Pretest-Posttest Experiment Survey Results (Mean & SD) – Group A

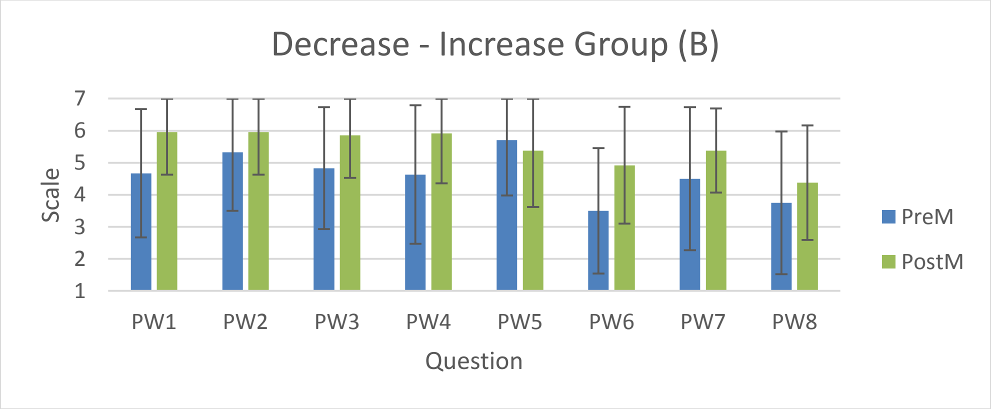


Figure 6b. Pretest-Posttest Experiment Survey Results (Mean & SD) – Group B

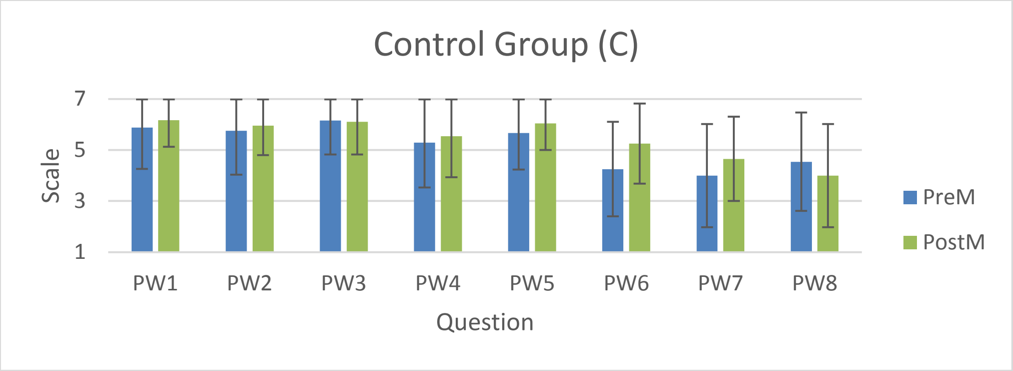


Figure 6c. Pretest-Posttest Experiment Survey Results (Mean & SD) – Group C

Quasi-Experiment

The second part of this study included completing a quasi-experiment. Similar to the pretest-posttest, the quasi-experiment was conducted with students selected from three Computer Concepts and Applications classes at a community college in the U.S. Data collection was completed cover the period from May 2015 to October 2015. The experiment required students to deploy virtual computers with the Windows 7 operating system and connected to a domain virtually. After the virtual machines were deployed, users had to logon to the computers at least once a week during the experiment. Once the users were logged on, they performed specific tasks such as logging to their email addresses from the Web, compose a new email, and send it with provided information to an email address, which was provided to them. After completing the tasks, the users logged off of the virtual machine. All their actions were anonymously recorded and the aggregated results are presented in Figure 6a-c.

Demographic Analysis

The demographic information for the users was solicited in the survey administered at the beginning of the experiment. In the quasi-experiment, the four variables of NFOLA, ALT, ATCT, and ARA were all controlled for computer experience, age, and gender. As such, it was necessary to collect the demographics of computer experience, age, and gender. Table 16 provides the demographic statistics data collected on the 71 respondents. Appendix D also shows the graphs of the demographics. From the data collected, about 58% reported that they have five or more years of computer experience, about 86% were in the 18-25 age group, and 62% were male students.

Table 16. Demographics Statistics of Study Participants (N=71)

Item	**Frequency**	**Percentage %**
Computer Experience (Years)		
0-1	8	11.3
2-5	22	31.0
6 & Up	41	57.7
Age		
18-25	61	85.9
26-49	9	12.7
50-69	1	1.4
Gender		
Male	44	62.0
Female	27	38.0

Pre-Analysis Data Screening (Quasi Experiment)

For the quasi-experiment, 75 users in three Computer Concepts and Applications classes were approached. 72 users consented to participate in the experiment and were given instructions for the experiment after completing the consent forms. The results of the four variables for the quasi-experiment were collected. Before the data analysis process could begin, a pre-analysis data screening was done. Levy (2006) has identified some reasons for the pre-analysis data screening to take place. The process of pre-analysis data screening was helpful in increasing the validity of the results as well as the accuracy of the data being analyzed. A visual inspection on the data was conducted to make sure that there was no missing data. Also as noted earlier, the Mahalanobis distance analysis was conducted and one multivariate outlier was removed.

Quasi-Experiment Data Analysis

The MANOVA test was used to assess group differences for the four variables of NFOLA, ALT, ATCT, and ARA. These tests were helpful in determining if there were any differences between the control group (C) and the increase-decrease password strength group (A), as well as the increase-increase password strength groups (B).

When it comes to NFOLA, ALT, ATCT, and ARA between Groups A, B, and Group C, the MANOVA results indicated that there was a significant difference between the groups. The F test, which was used, was the Wilk's Lambda. The Box's Test was evaluated first as significant ($p < 0.001$, $n=71$). The Wilk's Lambda indicated a significant mean group differences in the three groups with respect to NFOLA, ALT, ATCT, and ARA, Wilks' $\Lambda = .889$, $F(8, 1570) = 11.88$, $p < .001$, multivariate .057. Table 17 presents means and standards deviations for NFOLA, ALT, ATCT, and ARA by the group category.

Table 17. Means and Standard Deviations for Variables by Group

	NFOLA		ALT		ATCT		ARA	
Group	**M**	**SD**	**M**	**SD**	**M**	**SD**	**M**	**SD**
A	.44	.90	1.27	.60	2.09	.53	.08	.27
B	.41	.96	1.39	.68	2.01	.63	.10	.30
C	.05	.28	1.07	.27	1.86	.41	.00	.60

Figures 7a-d below also displays the graphs with the mean and standard deviations for NFOLA, ATL, ATCT, and ARA.

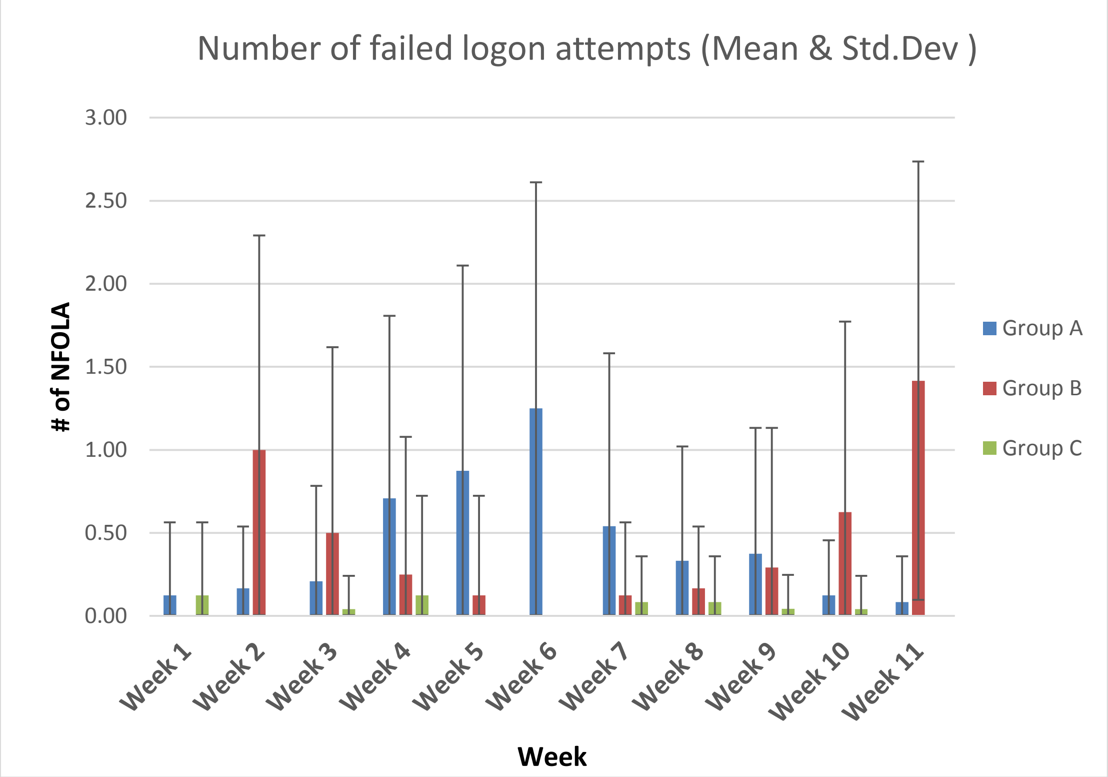


Figure 7a. NFOLA Mean and SD

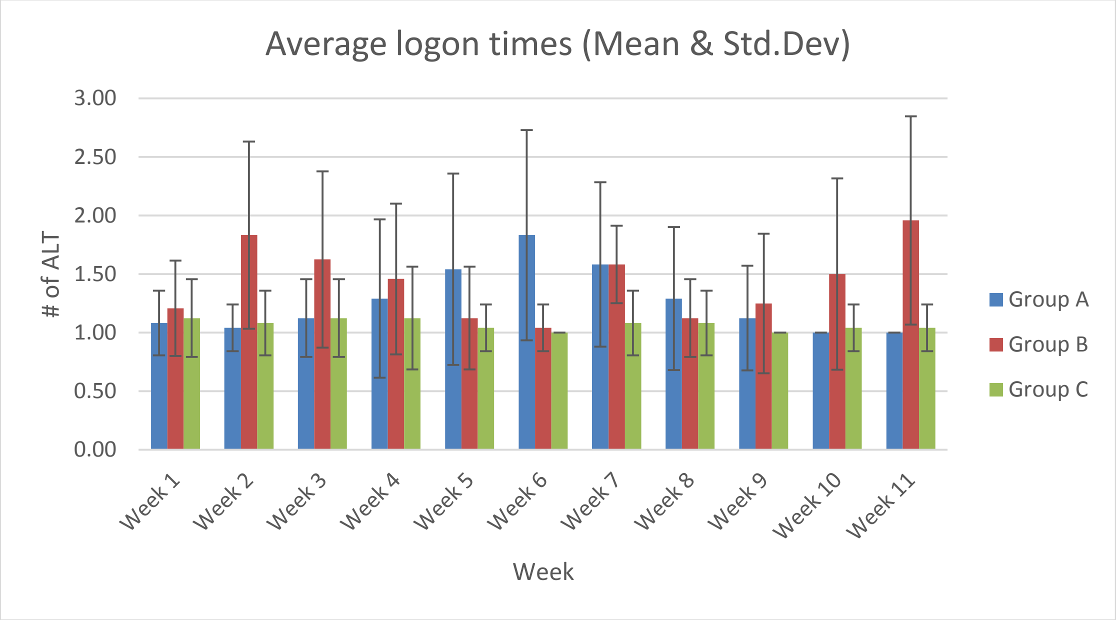


Figure 7b. ALT Mean and SD

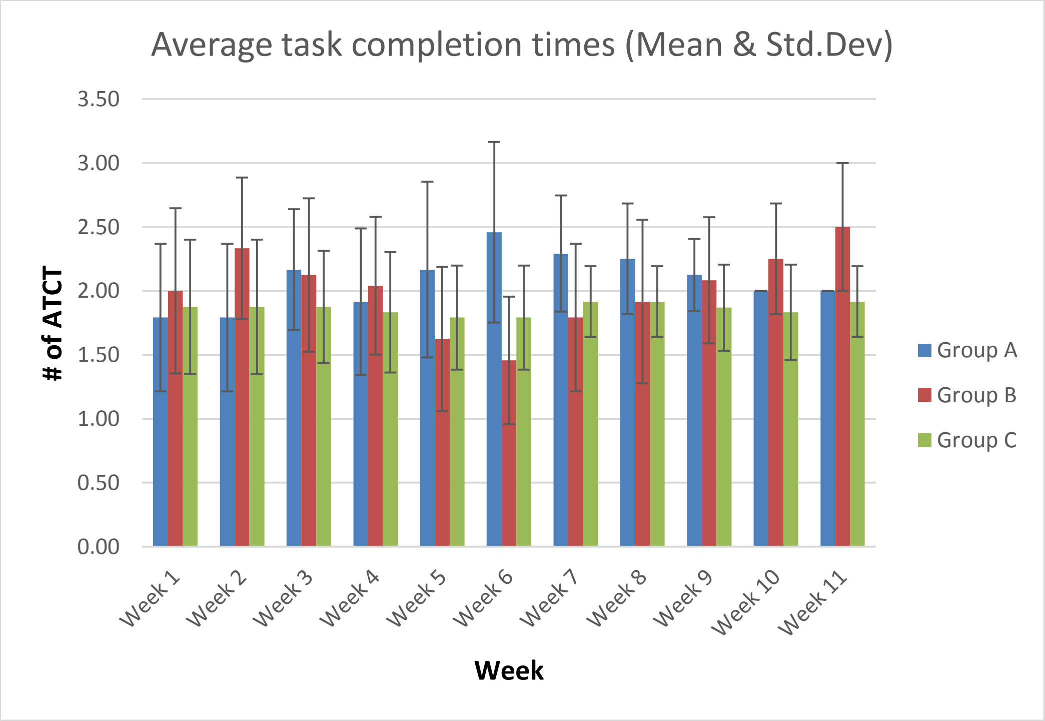


Figure 7c. ATCT Mean and SD

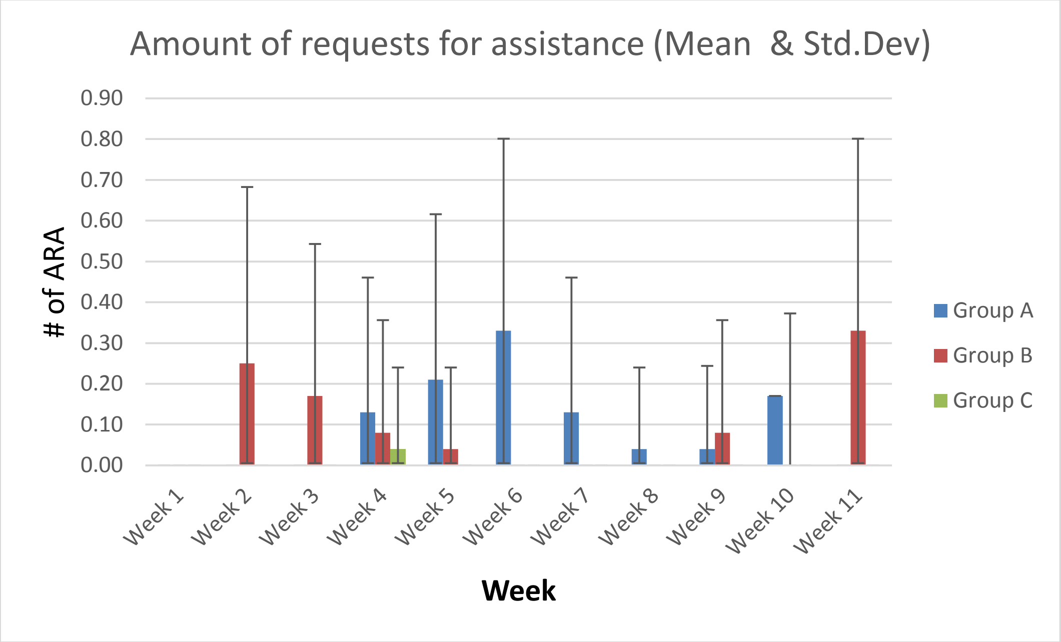


Figure 7d. ARA Mean and SD

Additionally, the MANCOVA was used to test the group differences on NFOLA, ALT, ATCT, and ARA when controlling for computer experience, gender, and age. As noted earlier, outliers were eliminated prior to the test. The preliminary or custom analysis was conducted to test the homogeneity of variance-covariance. The three covariates (computer experience, gender, & age) did not seem to influence group differences, the results are reported below.

The first covariate analyzed was computer experience. The MANCOVA results seem to suggest that the covariate of computer experience does not significantly influence the group differences, Wilks' Λ = .993, F (4, 784) = 1.36, p = .247, multivariate .007. When broken down by each variable, p = .17, .07, .96, .09 for NFOLA, ALT, ATCT, and ARA respectively. Table 18 shows the adjusted means (AM) and unadjusted means (UM) when controlling for computer experience.

Table 18. Adjusted and Unadjusted Means for Variables (Computer Experience)

	NFOLA		**ALT**		**ATCT**		**ARA**	
Group	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**
A	.43	.44	1.27	1.27	2.10	2.09	.08	.08
B	.42	.41	1.38	1.39	2.00	2.01	.10	.10
C	.47	.05	1.07	1.07	1.87	1.86	.00	.00

The second covariate analyzed was gender. The MANCOVA results seem to suggest that the covariate of gender does not significantly influence group differences, Wilks' Λ = .996, F (4, 820) = .82, p = .512, multivariate .004. When broken down by each variable, p = .32, .82, .91, .26 for NFOLA, ALT, ATCT, and ARA respectively. Table 19 shows the adjusted means (AM) and unadjusted means (UM) when controlling for gender.

Table 19. Adjusted and Unadjusted Means for Variables (Gender)

	NFOLA		**ALT**		**ATCT**		**ARA**	
Group	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**
A	.44	.44	1.27	1.27	2.09	2.09	.08	.08
B	.41	.41	1.39	1.39	2.00	2.01	.10	.10
C	.05	.05	1.07	1.07	1.86	1.86	.00	.00

The third covariate analyzed was age. The MANCOVA results seem to suggest that the covariate of age does not significantly influence group differences, Wilks' Λ =

.993, F (4, 784) = 1.34, p = .254, multivariate .007. When broken down by each variable, p = .53, .38, .03, .79 for NFOLA, ALT, ATCT, and ARA respectively. Table 20 shows the adjusted means (AM) and unadjusted means (UM) when controlling for age.

Table 20. Adjusted and Unadjusted Means for Variables (Age)

	NFOLA		**ALT**		**ATCT**		**ARA**	
Group	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**
A	.44	.44	1.27	1.27	2.09	2.09	.08	.08
B	.41	.41	1.39	1.39	2.01	2.01	.10	.10
C	.48	.05	1.07	1.07	1.86	1.86	.00	.00

Validity and Reliability Analysis

Trochim and Donnelly (2008) defined validity as the best available approximation to the truth of a given proposition, inference, or conclusion, while reliability was defined as repeatability and consistency. In this study, the pretest-posttest experiment survey with the control group design was used because of its strength in controlling threats to internal validity (Campbell & Stanley, 1963).

Straub (1989) mentioned internal validity as one that asks the question whether observed effects or results could have been caused by unmeasured variables. There were several threats to internal validity that were addressed in this study. The first one had to deal with users selecting the option of saving their passwords or writing them down. To ensure students did not have the ability to save passwords or write passwords down, students were instructed to put away all materials at the beginning of each session. The use of notebooks or any electronic devices was prohibited during the experiment. Active

Directory in Server 2008 was fully tested to ensure the authentication server was available during the experiment time and the password saving was not available.

External validity deals with how the results can be generalized to other settings or population (Sekeran, 2003). The study participants in this experimental study came from different majors as well as different academic levels, which was important in ensuring the results have implications for other groups and individuals in other settings as well as at other times (Staub, 1989). The tasks that the users performed during the experiment included: login to a computer, signing into an email account, composing an email message, sending the email with given data, signing out of the email account, and then login off the computer. The tasks were selected as they provided results, which are similar to the tasks that are performed by computer end users in real-world operational environments.

This study measured the point at which the increase of the cognitive load (via different password strength) becomes counterproductive to an organization and results were collected from NFOLA, ALT, ATCT, and ARA. Therefore, the study was successful in measuring what was intended to be measured thereby achieving the construct validity. The results of the study now make it possible to view when the effects of raising the cognitive load significantly differ among the three groups.

Summary of the Results

Chapter 4 reported on the results of this study. First, results of the pre-analysis of the pretest-posttest experiment survey were presented in Tables 14-5 as well as in Figure 6a-c. The data was screened for outliers and anomalies, which could have been a threat to the validity and reliability of the study. The results of the pre-analysis were presented in relevant tables.

The results of the pretest-posttest experiment survey analysis on 71 surveys from three groups indicated that there is a statistical difference between the user's perceptions about passwords before the quasi-experiment and after the quasi experiment (F = 1.210 and p = .029) among the groups. The results indicated that age and gender significantly affect user's perceptions about passwords.

A demographic analysis was also conducted. The demographic variables included: computer experience, gender, and age. The analysis was performed on the data collected from the pretest-posttest experiment surveys. The analysis revealed that out of the 71 users, about 58% reported that they have five and more years of computer experience, about 86% were in the 18-25 age group, and 62% were male students. Additionally, the quasi experiment data was analyzed to address all the hypotheses of this study. The Mahalanobis distance analysis on the data identified one multivariate outlier and it was removed from the data. The 71 cases remaining were then analyzed using MANOVA to test H1, H2, H3, and H4 hypotheses. The results indicated that there was a significant difference between the groups. The Wilk's Lambda indicated a significant group differences in the three groups with respect to the dependent variables of NFOLA, ALT, ATCT, and ARA, Wilks' Λ = .889, F(8, 1570) = 11.88, p < .001, multivariate .057.

Finally, the MANCOVA test was used to analyze the hypotheses H1a, H1b, H1c, H2a, H2b, H2c, H3a, H3b, H3c, H4a, H4b, and H4c. The results suggested that all three covariates of computer experience, gender, and age did not significantly influence the group differences of NFOLA, ALT, ATCT, and ARA, $p > .001$.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

This chapter begins by presenting the results from this study. The conclusions are presented as a review of the main goal and research questions that are the basis of the research. The findings as they relate to the hypotheses put forward in this study are also presented. The implications of the study are discussed followed by recommendations for future research. This chapter concludes with a general summary of this study.

The main goal of the research study was to assess the effect of changing the cognitive load (via different password strengths) over time on the number of failed operating system (OS) logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account), as well as assess the aforementioned relationships when controlled for age, gender, and computer experience. The main goal was achieved by addressing the following 16 hypotheses.

The first hypotheses (H1) was: *There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).* To address this hypotheses, a quasi-experiment was conducted to analyze data about the number of failed OS logon (NFOLA) attempts by three groups. A total of 71 users in three groups were examined as they were logging on the virtual computers. The treatment groups of A and B had 24 users each while the control group (C) had 23 students. The logs on a Server 2008 machine were recorded and analyzed for the three groups using MANOVA. The results revealed that at 95% confidence level. The mean NFOLA for Group A, B, and B were .44, .41, and .04 respectively. Therefore, the results indicated that there was a statistically significant difference (p < .001, n=71) between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group.

Hypotheses H1a was: *There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.* This hypotheses was analyzed using MANCOVA because of the control variable of computer experience. When controlling for computer experience, p = .167. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on NFOLA when controlling for computer experience.

Hypotheses H1b was: *There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.* This hypotheses was also analyzed using MANCOVA because of the control variable of computer experience. When controlling for age, p = .53. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on NFOLA when controlling for age.

Hypotheses H1c was: *There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.* When controlling for gender, p = .32. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on NFOLA when controlling for gender.

The second hypotheses (H2) was: *There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).* To address this hypotheses, a quasi-experiment was conducted to analyze data about the average logon times (ALT) by three groups. The time from the students were told to start and the time which the server indicated as authenticating users was recorded for all the users. The MANOVA test was also used to analyze the users average logon times. The mean times for ALT for all the three groups was recorded at 1.27, 1.39, and 1.07 for groups A, B, and C respectively. The results for the variable ALT also indicated that there was a statistically significant difference (p < .001, n=71) between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group.

Hypotheses H2a was: *There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-*

increase password strength group (B), and fixed password strength group (C) when controlling for computer experience. This hypotheses was analyzed using MANCOVA because of the control variable of computer experience. When controlling for computer experience, p = .07. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on ALT when controlling for computer experience.

Hypotheses H2b was: *There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.* This hypotheses was also analyzed using MANCOVA because of the control variable of computer experience. When controlling for age, p = .39. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on ALT when controlling for age.

Hypotheses H2c was: *There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.* When controlling for gender, p = .82. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on ALT when controlling for gender.

The third hypotheses (H3) was: *There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).* To address this hypotheses, a quasi-experiment was conducted to analyze data about the average task completion times (ATCT) by three groups. The ATCT was tracked from the time users were told to start the login process until the time they logged off. The time was calculated using the logs from Server 2008, recorded and then analyzed using MANOVA. For ATCT, the mean for group A, B, and C were 2.08, 2.01, and 1.86. The mean for the control group was lower as compared to the two treatment groups. The results for the variable ATCT also indicated that there was a statistically significant difference ($p < .001$, n=71) between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group.

Hypotheses H3a was: *There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.* This hypotheses was analyzed using MANCOVA because of the control variable of computer experience. When controlling for computer experience, $p = .96$. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on ATCT when controlling for computer experience.

Hypotheses H3b was: *There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-*

increase password strength group (B), and fixed password strength group (C) when controlling for age. This hypotheses was also analyzed using MANCOVA because of the control variable of computer experience. When controlling for age, p = .03. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on ATCT when controlling for age.

Hypotheses H3c was: *There will be no significant differences on the number of average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.* When controlling for gender, p = .91. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on ATCT when controlling for gender.

The fourth hypotheses (H4) was: *There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).* To address this hypotheses, a quasi-experiment was conducted to analyze data about the number of requests for assistance (ARA) by three groups. Active Directory in Server 2004 was used to set the account lockout threshold to 3 meaning that users would be locked out of the server after 3 failed logon attempts. For locked out users to be able to logon again, they had to request for assistance. The data was collected during the quasi-experiment. After the data was analyzed using MANOVA, the results showed that the mean for group A, B, and C were

.08, .1, and .00 respectively. The results for ARA also indicated that there was a statistically significant difference (p < .001, n=71) between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group.

Hypotheses H4a was: *There will be no significant differences on the number of requests for assistance between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.* This hypotheses was analyzed using MANCOVA because of the control variable of computer experience. When controlling for computer experience, p = .09. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on ARA when controlling for computer experience.

Hypotheses H4b was: *There will be no significant differences on the number of request for assistance between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.* This hypotheses was also analyzed using MANCOVA because of the control variable of computer experience. When controlling for age, p = .79. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on ARA when controlling for age.

Hypotheses H4c was: *There will be no significant differences on the number of request for assistance between the increase-decrease password strength group (A),* *decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.* When controlling for gender, p = .26. The results indicated that there was no statistically significant difference between the increase-decrease password strength group decrease-increase password strength group, and fixed password strength group on ARA when controlling for gender.

The four main hypotheses were rejected while all the when controlling for computer experience, gender and age were failed to reject. A summary of the hypotheses analysis is presented in Table 21.

Table 21. Summary of Null Hypothesis Analysis

	Hypothesis Analysis	
H1	There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).	Reject
H1a	There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.	Fail to Reject
H1b	There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.	Fail to Reject
H1c	There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.	Fail to Reject

H2	There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).	Reject
H2a	There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.	Fail to Reject
H2b	There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.	Fail to Reject
H2c	There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.	Fail to Reject
H3	There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).	Reject
H3a	There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.	Fail to Reject
H3b	There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.	Fail to Reject

H3c	There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.	Fail to Reject
H4	There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).	Reject
H4a	There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.	Fail to Reject
H4b	There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.	Fail to Reject
H4c	There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.	Fail to Reject

The results of this study answered the research questions which were previously asked as: At what point does the increase of the cognitive load (via different password strengths) become counterproductive to the organization by causing an increase in number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account)? The results reveal an increase in the number of filed OS logon attempts over the weeks with the highest in Week 5 and 6 for Group A as well a Week 10 and 11 for Group. The mean for the mentioned weeks are also at their highest level. Table 9a shows that the authentication strength for Group A is a passphrase with 15-20, 1 uppercase, 1 number, and two special characters in Week 5. Group B has the same strength in Week 10 as revealed in Table 9b. The results therefore suggest this is the point where users start having a sharp increase in NFOLA. Weeks 6 and 11 in Groups A and B respectively have the same authentication strength except that the characters in the passphrase are increased to 20-30 characters. The NFOLA is at its highest point in those weeks.

The ALT table reveal the average logon times increasing over the weeks as the authentication strength is raised for both Group A and B. The highest increase appear to be in Week 6 for Group A and Week 11 for Group B. The same pattern was also observed on the mean for ATCT and ARA. The mean for Group C which has an authentication strength of 7-10 characters, 1 uppercase, 1 number, and 1 special character stay about the same for NFOLA, ALT, ATCT, and ARA throughout the 11-week experiment time. It therefore appears that when the authentication strength is stronger than 7-10 characters, 1 uppercase, 1 number, and 1 special character it becomes counterproductive.

The second question was: At what point does such increase become counterproductive to the organization when controlled for computer experience, age and gender? The study answered this question in that results did not show any increases when the controlled for computer experience, age and gender.

Implications

This study has some implementations for the body of knowledge in the field of information systems.

Implications for Practice

The results makes noteworthy contributions to the body of knowledge, have implications for industry as well as for further study in the information systems domain. This study involved the observation and evaluation of the point at which an increase of the cognitive load (via different password strengths) become counterproductive to the organization by causing an increase in number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account). The study also examined the effects of controlling for computer experience, age, and gender.

The results of this study imply a number of points. The authentication strength increases, the number of failed logon attempts increases, average logon time increases, the amount of request for assistance due being locked out also increases. All the above increases lead to an increase of the average time they will take to complete tasks on the computer.

Implications for Research

While complex and long passwords are secure, there comes a point at which the complexity gets into the way of user's productivity. Other findings of this study further supports previous studies such as Crawford (2013), Henry (2007), Sridhar (2010), and Shay et al. (2010) that show negative results when a huge cognitive load is placed on the mind. The increase in authentication placed a higher cognitive load on the users which affected their ability to perform tasks.

There is an ongoing need in research of having secure systems which include strong passwords. As opportunities to implement and improve stronger authentication methods, it is important be to consider the limitations of the cognitive capabilities.

Study Limitations

There were some limitations which were experienced in this study. As noted in Chapter 1, this experiment was conducted at a medium sized two-year community college and participants will be undergraduate students pursuing an Associate degree. The study was also conducted over an 11-week period with users having to change their passwords every week.

Recommendations and Future Research

This research study was conducted at a two-year college. Future studies will be required to replicate the findings at other colleges and institutions as well as in industry. Four year colleges and institutions have a wider body of students when compared to a two-year college. Appendix D with the demographic charts show the majority of students in this study being in the 18-25 age range, performing a similar study with a wider frequency age is recommended.

As it relates to conducting this research over an 11-week period and changing the password every week, it may be meaningful to repeat the study over a longer period requiring users to change the passwords over a longer period than a week. Future studies could also explore the possibility of educating users on the benefits of security as it relates to passwords and authentication strength. While the pretest and posttest were used, there was no training or awareness about information security.

Summary

This research study addressed authentication problems that can be experienced by using the password method. The study tackled the obstacle of password memorability, which is further complicated by the fact that users have many passwords to recall for computers, networks, and Websites among other systems (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005). An infrequently used password that must be changed constantly, along with other security countermeasures, increases the cognitive load on users (Henry, 2007). This study observed one of the main ways used to authenticate users, which is through the use of passwords (Dasgupta & Saha, 2009).

The goals of this study was to find at what point does the increase of the cognitive load (via different password strengths) become counterproductive to the organization by causing an increase in number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account). Additional, the study had another goal of finding out at what point such increase becomes counterproductive to the organization when controlled for computer experience, age and gender. The following hypotheses were formed and addressed:

H1: There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H1a: There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.

H1b: There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.

H1c: There will be no significant differences on the number of failed OS logon attempts between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.

H2: There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H2a: There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.

H2b: There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.

H2c: There will be no significant differences on the average logon times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.

H3: There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H3a: There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.

H3b: There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.

H3c: There will be no significant differences on the average task completion times between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.

H4: There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H4a: There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for computer experience.

H4b: There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for age.

H4c: There will be no significant differences on the number of requests for assistance (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) when controlling for gender.

Based on the hypotheses and goals of this study, a pretest-posttest experiment survey and a quasi-experiment with three groups was employed. The three groups were the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C). The first two groups were treatment groups while the third one was a control group. There were 24 in the first two groups and 23 in the control group. The pretest experiment survey was administered to the students at the beginning of the study and the posttest survey was given at the end of the quasi-experiment. Users were then required to logon on virtual computer each week and perform given tasks like emailing weather information. As the users were logging onto the computer, their authentication strength was manipulated based on the group they belonged to. Group A and B had their authentication strength changed each week while that of Group C stayed the same. As they were logging in and performing the tasks during the quasi-experiment, the following was observed and tracked: number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account).

After the 11-week experiment, a pre-analysis data screening was conducted which resulted in one case being dropped as it was an outlier. The MANOVA test was used to test significant differences in the number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account) between group A, B and C. The tests found significant differences in all areas from participants in each group.

The MANCOVA test was used to test for significant differences in the number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock and reset account) between group A, B and C while controlling for computer experience, age, and gender. The results indicated there was no significant differences in the dependent variables between group A, B, and C while controlling for computer experience, age, and gender.

Appendix A

Pre-Experiment Survey

Instructions: Please complete the following survey by checking the most appropriate box for each question. The data collected will be used for research purposes and is not intended to be used for any other reason.

Computer User #____

What is your age range?

- □ 18-25
- □ 26-49
- □ 50-69
- □ 70 & Up

What is your gender?

- □ Male
- □ Female

How much computer experience do you have?

- □ 0-1
- □ 2-5
- □ 6 & Up

PW1. In general, I think it is very easy for me to remember my passwords
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW2. In general, the passwords I use are very easy for me to remember
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW3. I consider a password with over eight (8) characters (including at least1 uppercase, 1 letter, and 1 special character) to be strong
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW4. I use a password with eight (8) or more characters (including at least1 uppercase, 1 letter, and 1 special character) on most of my important accounts
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW5. I do not have problems with reusing the same password on multiple accounts
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW6. I feel comfortable with adapting to different requirements (e.g., a combination of letters and numbers vs. a combination of upper and lower case letters) furnished by password management systems.
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW7. When faced with a requirement to constantly change my password, I always write my password down (digitally or on paper)
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW8. I always use different complex passwords (eight (8) or more characters including at least 1 uppercase, 1 letter, and 1 special character) in my financial accounts.
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

Appendix B

Post Experiment Survey

Instructions: Please complete the following survey by selecting the most appropriate response for each question. Please note that your responses to this survey are completely anonymous and cannot be linked to you in any way. The information gathered will be used for research purposes only and is not intended to be used for any other reason.

PW1. I general, I think it is very easy for me to remember my passwords
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW2. I general, the passwords I use are very easy for me to remember
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW3. I consider a password with over eight (8) characters (including at least1 uppercase, 1 letter, and 1 special character) to be strong
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW4. I use a password with eight (8) or more characters (including at least1 uppercase, 1 letter, and 1 special character) on most of my important accounts

1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW5. I do not have problems with reusing the same password on multiple accounts
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW6. I feel comfortable with adapting to different requirements (e.g., a combination of letters and numbers vs. a combination of upper and lower case letters) furnished by password management systems.
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW7. When faced with a requirement to constantly change my password, I always write my password down (digitally or on paper)
1 – Strongly disagree
2 – Disagree
3 – Somewhat disagree
4 – Neither agree or disagree
5 – Somewhat agree
6 – Agree
7 – Strongly agree

PW8. I always use different complex passwords (eight (8) or more characters including at least 1 uppercase, 1 letter, and 1 special character) in my financial accounts.
1 – Strongly disagree
2 – Disagree

3 – Somewhat disagree

4 – Neither agree or disagree

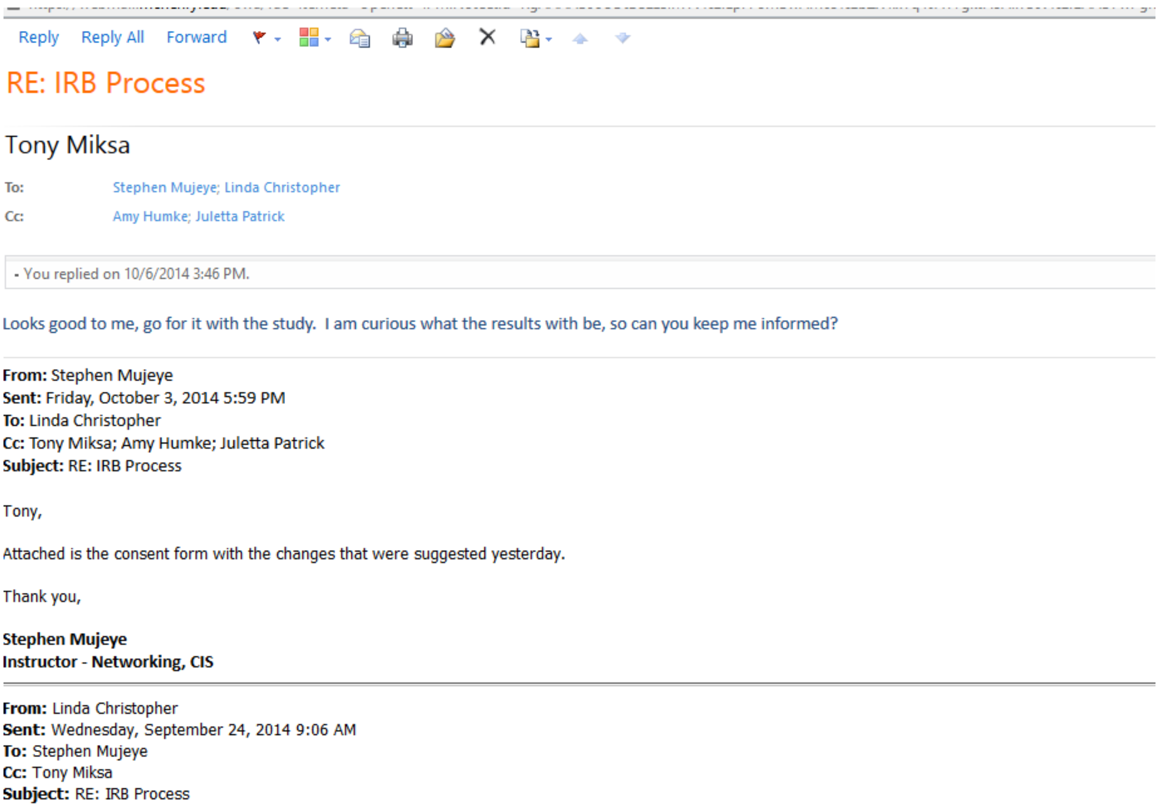
5 – Somewhat agree

6 – Agree

7 – Strongly agree

Appendix C

Approval Letter to Conduct Experiment at McHenry County College



RE: IRB Process

Tony Miksa

To: Stephen Mujeye; Linda Christopher

Cc: Amy Humke; Juletta Patrick

- You replied on 10/6/2014 3:46 PM.

Looks good to me, go for it with the study. I am curious what the results with be, so can you keep me informed?

From: Stephen Mujeye
Sent: Friday, October 3, 2014 5:59 PM
To: Linda Christopher
Cc: Tony Miksa; Amy Humke; Juletta Patrick
Subject: RE: IRB Process

Tony,

Attached is the consent form with the changes that were suggested yesterday.

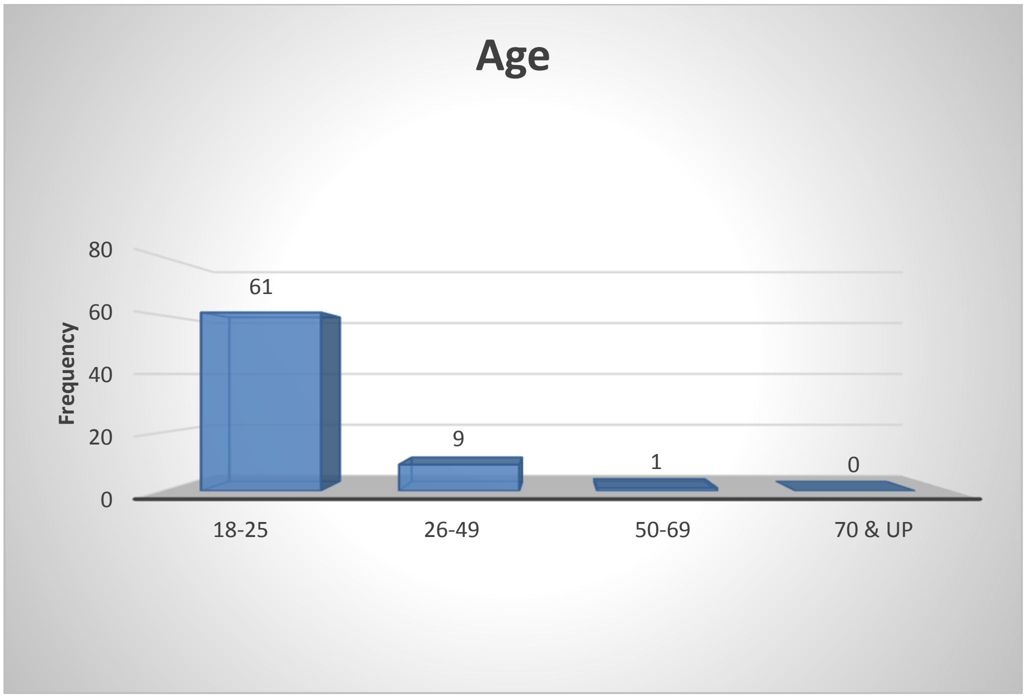
Thank you,

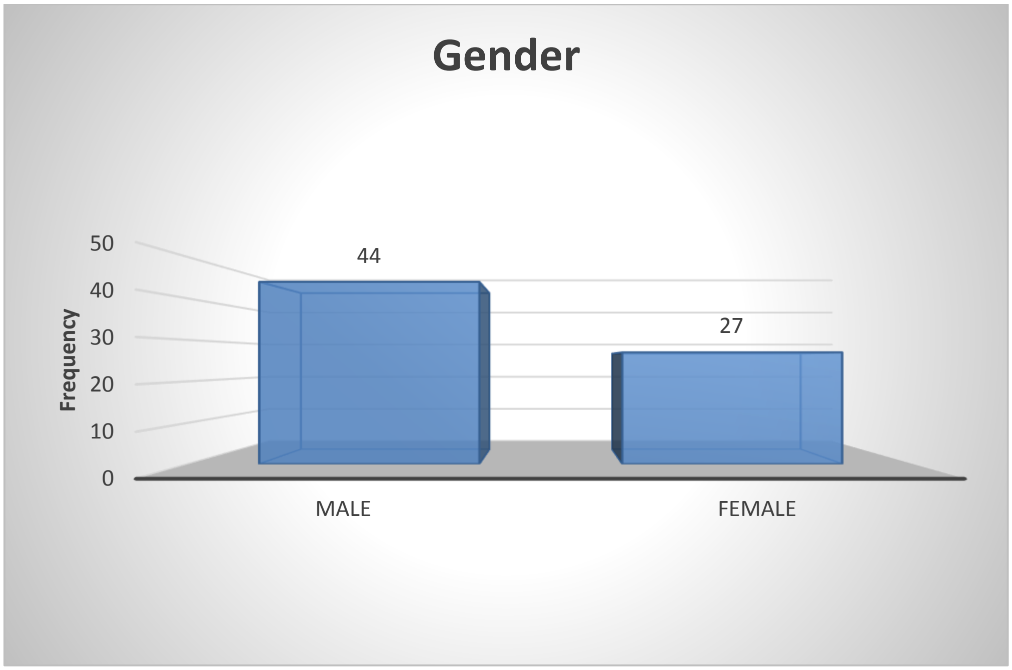
Stephen Mujeye
Instructor - Networking, CIS

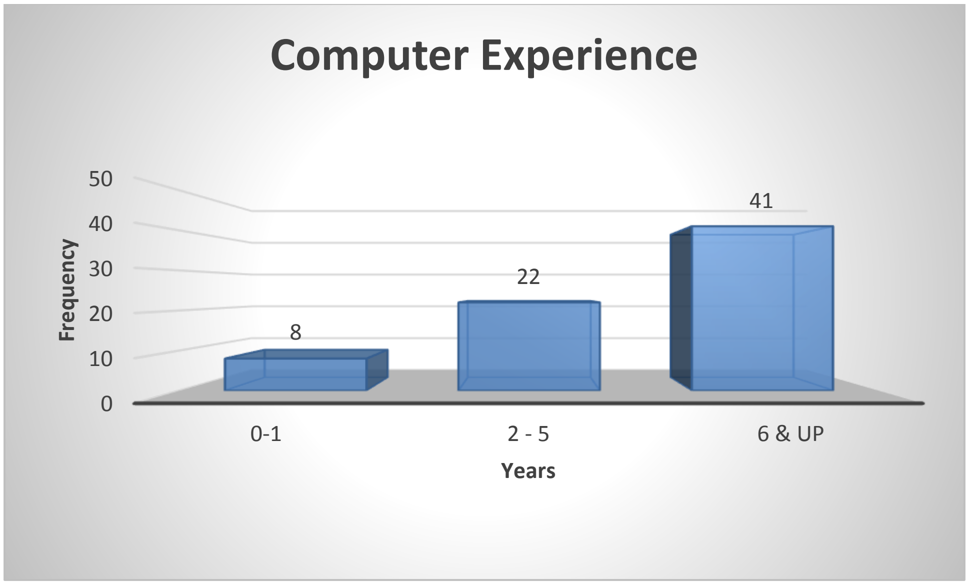
From: Linda Christopher
Sent: Wednesday, September 24, 2014 9:06 AM
To: Stephen Mujeye
Cc: Tony Miksa
Subject: RE: IRB Process

Appendix D

Demographic Statistics - Bar Charts






Computer Experience
Frequency
50
40
30
20
10
0
8
22
41
0-1
2 - 5
6 & UP
Years

References

Awwal, M. (2012). Influence of age and genders on the relationship between computer self-efficacy and information privacy concerns. *International Journal of Technology and Human Interaction, 8*(1), 14-37. doi:10.4018/jthi.2012010102

Banerjee, S., Kang, H., Bagchi-Sen, S., & Rao, H. (2005). Gender divide in the use of internet applications. *International Journal of E-Business Research, 1*(2), 24-39. doi:10.4018/jebr.2005040102

Banyal, R., Jain, P., & Jain, V. (2013). Multi-factor authentication framework for cloud computing. *Fifth International Conference on Computational Intelligence, Modelling and Simulation*, pp. 70-78.

Bard, M. (2007). Spelling-error tolerant, order-independent pass-phrases via the damerau-levenshtein string-edit distance metric. *Proceedings of the fifth Australasian symposium on ACSW frontiers*, Darlinghurst, Australia, pp. 117-124.

Benkhelifa, E., Fernando, D. A., & Welsh, T. (2013). A novel cloud-based multi-tenancy architecture with efficient hybrid authentication mechanism for enhanced security and resource optimization. *International Journal of Cloud Applications and Computing, 3*(3), 34-49. doi:10.4018/ijcac.2013070103

Biddle, R., Mannan, M., van Oorschot, P.C., & Whalen, T. (2011). User study, analysis, and usable security of passwords based on digital objects. *IEEE Transactions on Information Forensics and Security*, pp. 970 – 979.

Boechler, P. (2006). Understanding cognitive processes in educational hypermedia. *In C. Ghaoui (Ed.), Encyclopedia on Human Computers Interaction*, (648-651). Hershey, PA: Information Science Reference. doi:10.4018/978-1-59140-562-7.ch097

Brostoff, S., & Sasse, M. (2000). Are passfaces more usable than passwords? A field trial investigation. *Proceedings of the Human Computer Interactions Conference 2000*, London, UK, pp. 405-424.

Cahill, C. P., Martin, J., Phegade, V., Rajan, A., & Pagano, M. (2011). Client-based authentication technology: User-centric authentication using secure containers. *Proceedings of the Seventh ACM Workshop on Digital Identity Management*, New York, NY, pp. 83-92.

Campbell, D. T., & Stanley, J. C. (1963). *Experimental and quasi-experimental designs for research*. Hopewell, NJ: Houghton Mifflin Company.

Carstens, D., McCauley-Bell, P., Malone, L., & DeMara, R. (2004). Evaluation of the human impact of password authentication practices on information security. *Information Science Journal*, *7*(1), 67-85.

Cassini, J. A., Medlin, B., & Romaniello, A. (2008). Laws and regulations dealing with information security and privacy: An investigative study. *International Journal of Information Security and Privacy, 2*(2), 70-82. doi:10.4018/jisp.2008040105

Chakrabarti, S. & Singbal, M. (2007). Password-based authentication: preventing dictionary attacks. *IEEE Computer Society, 40* (6), 68-74.

Chaudhari, S., Tomar, S., & Rawat, A. (2011). Design, implementation and analysis of multi layer, multi factor authentication (MFA) setup for webmail access in multi trust networks. *International Conference on Emerging Trends in Networks and Computer Communications*, pp. 27-32.

Chiasson, S., Forget, A., Stobert, E., van Oorschot, P. C., & Biddle, R. (2009). Multiple interference in text passwords and click-based graphical passwords. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Swinton, UK, pp. 500-511.

Chilton, M. A., & Gurung, A. (2008). Management of lecture time: using the web to manipulate extrinsic cognitive load. *International Journal of Web-Based Learning and Teaching Technologies*, *2*(3), 35-47. doi:10.4018/jwltt.2008040103

Choi, Y., Lee, D., Kim, J., Jung, J., & Won, D. (2015). Cryptanalysis of improved biometric-based user authentication scheme for C/S system. *International Journal of Information and Education Technology, 5*(7), 538-542. doi:http://dx.doi.org/10.7763/IJIET.2015.V5.564

Chudá, D., & Ďurfina, M. (2009). Multifactor authentication based on keystroke dynamics. *Proceedings of the International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing*, pp. 1 – 6.

Ciampa, M. (2012). *Security+ Guide to network security fundamentals* (4th ed.). Boston. MA: Course Technology

Costabile, M. F., Fogli, D., & Lanzilotti, R. (2006). Supporting work practice through end-user development environments. *Journal of Organizational and End User Computing (JOEUC), 4*(18), 43-65. doi:10.4018/joeuc.2006100103

Corbató, F. J., Merwin-Daggett, M., & Daley, R. (1962). An experimental time-sharing system. *Proceedings of the Spring Joint Computer Conference,* pp. 335-344.

Crawford, J. (2013). Assessing the value of formal control mechanisms on strong password selection. *International Journal of Secure Software Engineering, 4*(3), 1-17. doi:10.4018/jsse.2013070101

Czeskis, A., Dietz, M., Kohno, T., Wallach, D., & Balfanz, D. (2012). Strengthening user authentication through opportunistic cryptographic identity assertions. *Proceedings of the 2012 ACM conference on Computer and Communications Security*, pp. 404-414.

Dean, T. (2010). *Network+ guide to networks*. (5th ed.). Boston, MA: Course Technology.

Delic, K. A., & Hoellmer, B. (2000). Knowledge-based support in help-desk environments. *IEEE Computer Society, 2* (1), 44-48.

Dossogne, J., & Lafitte, F. (2013). On authentication factors: "What you can" and "how you do it". *Proceedings of the 6th International Conference on Security of Information and Networks*, Brussels, Belgium, pp. 70-78.

Erlich, Z., & Zviran, M. (2010). Goals and practices in maintaining information systems security. *International Journal of Information Security and Privacy, 4*(3), 40-50. doi: 10.4018/jisp.2010070103

Erlich, Z., & Zviran, M. (2009). Authentication methods for computer systems security. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology, Second Edition* (pp. 288-293). Hershey, PA: Information Science Reference. doi:10.4018/978-1-60566-026-4.ch049

Fan, L., & Lei, M. (2008). Reducing cognitive overload by meta-learning assisted algorithm selection. *International Journal of Cognitive Informatics and Natural Intelligence, 3*(2), 90-100. doi:10.4018/jcini.2008070107

Gearhart, D. (2010). The issues related to student authentication in distance education. *International Journal of Technoethics, 1*(1), 60-69. doi:10.4018/jte.2010081005

Grawemeyer, B., & Johnson, H. (2011). Using and managing passwords: a week to view. *Interacting with computers, 23*(3), 256-267. doi:10.1016/j.intcom.2011.03.007

Gross, T. (2003). Security analysis of the SAML single sign-on browser/artifact profile. *Proceedings of the 19th Annual Computer Security Applications Conference*, pp. 298-307.

Gunson, N., Marshall, D., McInnes, F., Morton, H., & Jack, M. (2014). Usability evaluation of dialogue designs for voiceprint authentication in automated telephone banking. *International Journal of Technology and Human Interaction, 2*(10), 59-77. doi:10.4018/ijthi.2014040104

Harby, F. A., Qahwajim, R., & Kamala, M. (2010). Towards an understanding of user acceptance to use biometrics authentication systems in e-commerce: Using an extension of the technology acceptance model. *International Journal of E-Business Research, 6*(3), 34-55. doi:10.4018/jebr.2010070103

Hernández-López, A., Colomo-Palacios, R., García-Crespo, Á., & Cabezas-Isla, F. (2011). Software engineering productivity: Concepts, issues and challenges. *International Journal of Information Technology Project Management (IJITPM), 2*(1), 37-47. doi:10.4018/jitpm.2011010103

Henry. P. T. (2007). *Toward usable, robust memometric authentication: An evaluation of selected password generation assistance.* Dissertation Abstracts International, 68 (09), (UMI No. AAT 3282618). Retrieved March 31, 2013 from Digital Dissertations database.

Herley, C. (2009). So long and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the New Security Paradigms Workshop*, Oxford, UK, pp. 1-12.

Herley, C., Oorschot, P., & Patrick A. (2009). Passwords: If we're so smart, why are we still using them? *International Conference on Financial Cryptography and Data Security*, Accra Beach, Barbados, pp. 1-8.

Hogg, N. (2007). Measuring cognitive load. In R. Reynolds, R. Woods, & J. Baker (Eds.), *Handbook of Research on Electronic Surveys and Measurements* (pp. 188-194). Hershey, PA: doi:10.4018/978-1-59140-792-8.ch020

Hoxmeier, J., Nie, W., & Purvis, G. (2000). The Impact of gender and experience on user confidence in electronic mail. *Journal of Organizational and End User Computing, 12*(4), 11-20. doi:10.4018/joeuc.2000100102

Huang X., Xiang Y., Bertino E., Zhou J., & Xu L. (2014). User study, analysis, and usable security of passwords based on digital objects. *IEEE Transactions on Dependable and Secure Computing*, pp. 568 – 581. doi: 10.1109/TDSC.2013.2297110

Hussain, A. K., & Alnabhan, M. M. (2014). Advanced authentication scheme using a predefined keystroke structure. *International Journal of Computer Science & Information Technology, 6*(2), 163-169.

Hussein, I. S. H., & Nordin, M. J. (2014). Palmprint verification using invariant moments based on wavelet transform. *Journal of Computer Science, 10*(8), 1389-1396

Hwang, J., Wu, K., & Liu D. (2000). Access control with role attribute certificates. *Computer Standards & Interfaces, 22*(1), 43-53

Inglesant, P., & Sasse, M. (2010). The true cost of unusable password policies: password use in the wild. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* New York, NY, pp. 383-392.

Iwai, K., Iida, K., Akiyoshi, M., & Komoda, N. (2010). A help desk support system with filtering and reusing E-mails. *IEEE International 8th Conference on Industrial Informatics,* Osaka, Japan, pp. 321-325.

Jenkins, J. L., Durcikova, A., & Burns, M. B. (2013). Simplicity is bliss: Controlling extraneous load in online security training to promote secure behavior. *Journal of Organizational and End User Computing, 3*(25), 52-66. doi:10.4018/joeuc.2013070104

Jung, J., Choi, Y., Lee, D., Kim, J., & Won, D. (2015). Security weaknesses of a timestamp-based user authentication scheme with smart card. *International Journal of Information and Education Technology, 5*(7), 553-556. doi:http://dx.doi.org/10.7763/IJIET.2015.V5.567

Kane, K., & Browne J. (2006). On classifying access control implementations for distributed systems. *Proceedings of the eleventh ACM symposium on Access control models and technologies,* New York, NY, pp. 29-38.

Keith, M., Shao, B., & Steinbart, P. J. (2007). The usability of passphrases for authentication: an empirical field study. *International Journal of Human-Computer Studies*, *65*(2007), 17-28.

Kim, I. (2012). Keypad against brute force attacks on smartphones. *Journal of Institution of Engineering and Technology. 6*(2), 71-76.

Kinsbourne, M., & George, J. (1974). The mechanics of the word frequency effect on recognition memory. *Journal of Verbal Learning and Verbal Behavior,* 13, 63-69.

Kline, D., He, L., & Yaylacicegi, U. (2011). User perceptions of security technologies. *International Journal of Information Security and Privacy, 5*(2), 1-12. doi:10.4018/jisp.2011040101

Kumari, K., & Chithraleka, T. (2012). A comparative analysis of access control policy modeling approaches. *International Journal of Secure Software Engineering, 3*(4), 65-83.

Lee, L., Kim, Y., & Lee, S. (2001). The influences of media choice on help desk performance perception. *Proceedings of the 34th Hawaii International Conference on System Sciences,* Maui, HI, pp.1-7.

Lehtonen, M.O., Michahelles, F., & Fleisch, E. (2007). Trust and security in RFID-based product authentication systems. *IEEE Systems Journal*, *(1)* 2, 129-144.

Levy, Y. (2006). *Assessing the value of E-learning systems.* Hershey, PA: Information Science Publishers.

Levy, Y., & Ellis, T. (2011). A guide for novice researchers on experimental and quasi-experimental studies in information systems research. *Interdisciplinary Journal of information, knowledge, and management*, 6, 151-161.

Levy, Y., Ramim, M. M., Furnell, S. M., & Clarke, N. L. (2011). Comparing intentions to use university-provided vs. vendor-provided multibiometric authentication in online exams. *Campus-Wide Information Systems, 28*(2), 102-113. doi:10.1108/10650741111117806

Lutu, P. E. (2005). Database sampling for data mining. In J. Wang (Ed.), *Encyclopedia of Data Warehousing and Mining* (pp. 344-348). Hershey, PA: doi:10.4018/978-1-59140-557-3.ch066

Ma, Y., & Feng F. (2011). Evaluating usability of three authentication methods in web-based application. *9th International Conference on Software Engineering Research, Management and Applications,* pp. 81-88.

Maguire, J. & Renaud, K. (2012). You only live twice or "the years we wasted caring about shoulder-surfing". *Proceedings of the 26th Annual BCS Interaction Specialist Group Conference on People and Computers*, pp. 404-409.

Marnell, J. W., & Levy, Y. (2013). Towards a model of factors affecting resistance to using multi-method authentication. *Information Security Education Journal, 1*(1), 37-45.

Marthandan, G., & Meng, T. C. (2010). Thirst for business value of information technology. *International Journal of Technology Diffusion, 1*(1), 28-40.

Mattord, H. J. (2012). *Assessment of web-based authentication methods in the U.S.: Comparing E-learning systems to internet healthcare information systems.* (Order No. 3526070, Nova Southeastern University). *ProQuest Dissertations and Theses,* 156. Retrieved from http://search.proquest.com.ezproxylocal.library.nova.edu/docview/1115135156?accountid=6579. (1115135156).

Mattord, H. J., Levy, Y., & Furnell, S. (2013). An expert panel approach on developing a unified system authentication benchmarking index. *International Journal of Interdisciplinary Telecommunications and Networking, 5*(2), 32-42. doi:10.4018/jitn.2013040103

McCloskey, D. W., & Leppel, K. (2010). The impact of age on electronic commerce participation: An exploratory model. *Journal of Electronic Commerce in Organizations*, *8*(1), 41-60. doi:10.4018/jeco.2010103003

McMillan, R. (2012, January 27). Re: The world's first computer password? It was useless too. Retrieved from http://www.wired.com/2012/01/computer-password

Medlin, B. D. (2013). Social engineering techniques and password security: Two issues relevant in the case of health care workers. *International Journal of Cyber Warfare and Terrorism*, *2*(3), 58-70. doi:10.4018/ijcwt.2013040104

Medlin, B. D., & Cazier, J. A. (2007). An empirical investigation: Health care employee passwords and their crack times in relationship to HIPPA security standards. *International Journal of Healthcare Information Systems and Informatics*, *2*(3), 39-48.

Meng, K. (2012). Designing click-draw based graphical password scheme for better authentication. *IEEE Seventh International Conference on Networking, Architecture, and Storage*, Fujian, China, pp. 39-48.

Menkus, B. (1998). Understanding the use of passwords. *Computers & Security*, *7*(2), 132-136.

Mertler, C., & Vanatta, R. (2010). *Advanced and multivariate statistical methods: Practical application and interpretation* (4th ed.). Los Angeles: Pyrczak.

Mihajlov, M., & Blazic, B. J. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. *Interacting with Computers*, *23*(2011), 582-593.

Miller, A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, *63*, 81-97.

Millhouse, C. (1999). Workgroup help desk software: Making sense of the market. *Service News*, *19*(2), 33-35. Retrieved from http://search.proquest.com.ezproxylocal.library.nova.edu/docview/221105497?accountid=6579

Mittal, N., & Nault, B. (2009). Investments in information technology: indirect effects and information technology intensity. *Information Systems Research*, *20*(1), 140-154.

Molloy, I., & Li, N. (2011). Attack on the gridcode one-time password. *Proceedings of the 6th ACM symposium on information, computer and communications security*, New York, NY, pp. 306-315.

Nachum, L. (1999). Measurement of productivity of professional services. *International Journal of Operations & Production Management*, *9*(9/10), 922–950. doi:10.1108/01443579910280269

Nashwan, S., & Alshammari, B. (2014). Mutual chain authentication protocol for SPAN transactions in Saudi Arabian banking. *International Journal of Computer and Communication Engineering, 3*(5), 326-333. doi:http://dx.doi.org/10.7763/IJCCE.2014.V3.344

Natarajan, T., Rajah, S. R., & Manikavasagam, S. (2011). Snapshot of personnel productivity assessment in Indian IT industry. *International Journal of Information Technology Project Management*, *2*(1), 48-61. doi:10.4018/jitpm.2011010104

Ngugi, B., & Kamis, A. (2013). Modeling the impact of biometric security on millennials' protection motivation. *Journal of Organizational and End User Computing, 4*(25), 27-49. doi:10.4018/joeuc.2013100102

Ngugi, B., Tarasewich, P., & Recce, M. (2012). Typing biometric keypads: combining keystroke time and pressure features to improve authentication. *Journal of Organizational and End User Computing (JOEUC), 1*(24), 42-63. doi:10.4018/joeuc.2012010103

Novakovic, L., McGill, T., & Dixon, M. (2009). Understanding user behavior towards passwords through acceptance and use modeling. *International Journal of Information Security and Privacy*, *3*(1), 11-29.

Oreku, G., & Lin J. (2009). End user authentication (EUA) model and password for security. *Journal of Organizational and End User Computing*, *21*(2), 28-33.

Paas F., & Kester, L. (2006). Learner and information characteristics in the design of powerful learning environments. *Applied Cognitive Psychology*, 20(3), 281-285.

Rane, S. & Sun W. (2010) Privacy preserving string comparisons based on Levenshtein distance. *Information Forensics and Security (WIFS), 2010 IEEE International Workshop*, Seattle, WA, pp. 1-6. doi: 10.1109/WIFS.2010.5711449

Ren, X., & Wu, X. (2012). A novel dynamic user authentication scheme. *International Symposium on Communications and Information Technologies*, Gold Coast, Queensland, Australia, pp. 713-717.

Revett, K. (2009). A bioinformatics based approach to user authentication via keystroke dynamics. *International Journal of Control, Automation and Systems*, *7*(1), 7–15.

Sasse, M., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' – a human/computer interaction approach to usable and effecting security. *Technology Journal*, *19*(3), 122-131.

Sayoud, H. (2011). Biometrics: An Overview on new technologies and ethic problems. *International Journal of Technoethics, 1*(2), 19-34. doi:10.4018/jte.2011010102

Sekaran, U. (2003). *Research methods for business: A skill building approach* (4th ed.). New York: John Wiley & Sons, Inc.

Shay, R., & Bertino, E. (2009). A comprehensive simulation tool for the analysis of password policies. *International Journal of Information Security, 8*(4), 275-289. DOI 10.1007/s10207-009-0084-3

Shay, R., Komanduri, S., Kelly, P., Leon, P., Mazurek, M., Bauer, L., Christin, N., & Cranor, L. (2010). Encountering stronger password requirements: User attitudes and behaviors. *Symposium on Usable Privacy and Security.* Redmond, WA, pp. 1-20.

Shoemaker, D., & Sigler, K. (2015). *Cybersecurity engineering a secure information technology organization*. Stamford, CT: Course Technology.

Sridhar, V. (2010). Challenges of information security management in a research and development software services company: Case of wirelessComSoft. *Journal of Cases on Information Technology, 12*(2), 16-30. doi:10.4018/jcit.2010040102

Straub, D. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.

Sweller, J. (1988). Cognitive load during problem solving: Effect on learning. *Cognitive Science*, 12, 257-285.

Thomas, S. (2009). Making help desk training interactive and interesting for student technicians. *Proceedings of the 37th Annual ACM SIGUCCS Fall Conference, New York, NY, pp. 249-252.*

Tiwari, P.B., & Joshi, S.R. (2009). Single sign-on with one time password. *IEEE Seventh International Conference on First Asian Himalayas*, pp. 1-4.

Trochim, W., & Donnelly, J. (2008). *The research methods knowledge base* (3rd ed.). Mason: Cengage Learning.

Tsai, C., Lee, C., & Hwang, M. (2006). Password authentication schemes: Current status and key issues. *International Journal of Network Security, 3*(2), 101-115.

Vu, K., Proctor, R., Spantzel, A., B., Tai, B., Cook, J., & Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, *65*(2007), 744-757. doi:10.1016/j.ijhcs.2007.03.007

Wang, S., & Wang H. (2008). Password authentication using hopfield neural networks. *IEEE Transactions on Applications and Reviews*, pp. 265 – 269.

Wang, D., He, D., Wang, P., & Chu, C. (2014). Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. *IEEE Transactions on Dependable and Secure Computing*, pp. 1-14.

Warkentin, M., Davis, K., & Bekkering, E. (2004). Introducing the check-off password system (COPS): An advancement in user authentication methods and information security. *Journal of Organizational and End User Computing, 16*(3), 41-58. doi:10.4018/joeuc.2004070103

Weihrich, H., & Koontz, H. (1994). *Management: A global perspective*. New York: McGraw-Hill.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). PassPoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, *63*(1-3), 102-127. doi:10.1016/j.ijhcs.2005.04.010

Whitman, M. & Mattord, H. (2016). *Principles of information security*. (5th ed.). Boston, MA: Course Technology.

Wierschem, D. C., & Brodnax, T. L. (2003). The impact of computer processor speed on end-user productivity. *Journal of Organizational and End User Computing),* *15*(2), 23-36. doi:10.4018/joeuc.2003040102

Wiggins, C. (2012). Self-service portal solves the forgotten password dilemma. *Proceedings of the 40th Annual ACM SIGUCCS Conference on User Services,* New York, NY, pp. 127-130.

Wong, J., & Down, K. (2011). The effects of investments in information technology on firm performance: An investor perspective. *Journal of Information Technology Research*, *4*(3), 1-13.

Xiao, Y., Li, C., Lei, M., & Vrbsky, S. (2014). Differentiated virtual passwords, secret little functions, and codebooks for protecting users from password theft. IEEE *Systems Journal*, *8*(2), 406-416. DOI: 10.1109/JSYST.2012.2183755

Yi, M. Y., & Im, K. S. (2004). Predicting computer task performance: Personal goal and self-efficacy. *Journal of Organizational and End User Computing, 16*(2), 20-37. doi:10.4018/joeuc.2004040102

Yu, J., Wang, G., Mu, Y., & Gao, W. (2014). An efficient generic framework for three-factor authentication with provably secure instantiation. *IEEE Transactions on Information Forensics and Security*, pp. 2302 – 2313.

Zviran, M., & Haga, W. (1999). Password security: An empirical study. *Journal of Management Information Systems*, *15*(4), 161-184.