2016

An Empirical Study of Authentication Methods to Secure E-learning System Activities Against Impersonation Fraud

Shauna Beaudin

Nova Southeastern University, sb1324@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.

Share Feedback About This Item

An Empirical Study of Authentication Methods to Secure E-learning System
Activities Against Impersonation Fraud

by

Shauna Beaudin

A dissertation submitted in 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 Shauna Beaudin, 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.   Date
Chairperson of Dissertation Committee

_____   _____
Theon Danet, Ph.D.   Date
Dissertation Committee Member

_____   _____
James Parrish, Ph.D.   Date
Dissertation Committee Member

Approved:

_____   _____
Amon B. Seagull, Ph.D.   Date
Interim Dean, College of Engineering and Computing

College of Engineering and Computing
Nova Southeastern University
2016

An Empirical Study of Authentication Methods to Secure E-learning System Activities Against Impersonation Fraud

by
Shauna Beaudin
March 2016

Studies have revealed that securing Information Systems (IS) from intentional misuse is a concern among organizations today. The use of Web-based systems has grown dramatically across industries including e-commerce, e-banking, e-government, and e-learning to name a few. Web-based systems provide e-services through a number of diverse activities. The demand for e-learning systems in both academic and non-academic organizations has increased the need to improve security against impersonation fraud. Although there are a number of studies focused on securing Web-based systems from Information Systems (IS) misuse, research has recognized the importance of identifying suitable levels of authenticating strength for various activities. In e-learning systems, it is evident that due to the variation in authentication strength among controls, a 'one size fits all' solution is not suitable for securing diverse e-learning activities against impersonation fraud.

The main goal of this study was to use the framework of the Task-Technology Fit (TTF) theory to conduct an exploratory research design to empirically investigate what levels of authentication strength users perceive to be most suitable for activities in e-learning systems against impersonation fraud. This study aimed to assess if the 'one size fits all' approach mainly used nowadays is valid when it comes to securing e-learning activities from impersonation fraud. Following the development of an initial survey instrument (Phase 1), expert panel feedback was gathered for instrument validity using the Delphi methodology. The initial survey instrument was adjusted according to feedback (Phase 2). The finalized Web-based survey was used to collect quantitative data for final analyses (Phase 3).

This study reported on data collected from 1,070 e-learners enrolled at a university. Descriptive statistics was used to identify what e-learning activities perceived by users and what users perceived that their peers would identify to have a high potential for impersonation. The findings determined there are a specific set of e-learning activities that high have potential for impersonation fraud and need a moderate to high level of authentication strength to reduce the threat. Principal Component Analysis was used to identify significant components of authentication strength to be suitable against the threats of impersonation for e-learning activities.

Acknowledgments

This dissertation has been one of the most intense endeavors of my life. I am incredibly fortunate to be surrounded by so many remarkable people who were with me throughout this experience. To all of you, I have so much gratitude for generous your support.

First, I want to express my deepest appreciation to my dissertation committee chair, Dr. Levy. This accomplishment would not have been possible without you. Your patience and knowledge were invaluable and I am forever thankful. Every critique was essential and encouraged me to improve my research. Your dedication was immeasurable and I am honored that I got to work with you. I also want to thank my committee members, Dr. Danet and Dr. Parrish, for taking the time to review my research and provide comments that were instrumental to the progress of this dissertation.

For my parents, Ray and Leona, I want to thank you from the bottom of my heart for your unwavering faith in me to succeed in all that I do. You have given me so much love, support, and guidance throughout my life. It is because of you I had the strength and commitment to complete this goal.

For my husband, Joe, you were the one by my side through this entire journey. I am sincerely grateful for all the encouragement you provided each and every day. The sacrifices you made for me while I was completing my research made it possible for me to keep moving forward. For my children, Lauren and Jacob, I am proud of you every day. You were both so understanding when I could not be with you because I had to write. My brother-in-law, John, gets a special thank you for always being available to help with the children when I was required to travel. Thank you all for filling my life with love and fun.

Finally, there are a number of friends who were there for me whenever I needed them. Ellen, Karen, and Sonja, you are truly genuine friends. Thank you for helping me maintain my sanity when I was trying to keep my life balanced throughout this process.

Table of Contents

List of Tables

Tables

List of Figures

Chapter 1

Introduction

Background

This study was concerned with the issue of securing Web-based systems against

impersonation and the identification of suitable authentication controls for e-learning

activities with high potential of impersonation (Apampa, Wills, & Argles, 2010). Helkala

and Snekkenes (2009) defined suitable authentication as, "an authentication product that

must comply with usage and environment-related requirements dictated by the scenario"

(p. 4). Control is defined by Van Aken (1978) as, "the use of interventions by a controller

to promote a preferred behavior of a system being controlled" (p. 44). Suitable

authentication controls allow organizations to achieve its security goals by assessing the

value of the activity and identifying the threat for the activity being protected (Apampa et

al., 2010).

E-learning uses a wide range of learning activities to meet learning outcomes via the

Internet, commonly known as Web-based systems. In addition to the prevalent use within

academic institutions, organizational use of e-learning systems as a means to train

employees has grown where more than two-thirds of employers use e-learning systems

for testing alone (Makransky & Glas, 2011). Due to the increase in demand for e-learning

via Web-based systems (e-learning systems), the need to improve security has equally

increased (Aceves & Aceves, 2009). Regulations have been created such as The Higher

Education Opportunity Act (HEOA), which requires institutions who offer e-learning to strengthen their practices for authenticating e-learners (Aceves & Aceves, 2009).

A number of differing solutions have been proposed to address this prevailing issue by using authentication controls with a wide variation of strength, however, there is a lack of consistency in what level of authentication strength is suitable (Jalal & Zeb, 2008). Penteado and Marana (2009) used facial recognition to authenticate users continuously throughout the use of an e-learning activity. Levy and Ramim (2010) studied the acceptance of multi-biometric authentication in e-learning systems such as facial recognition, keystroke patterns, and fingerprint recognition. Ibrahim, Ali, and Nassr (2011) studied the use of continuous biometric techniques such as facial recognition, voice recognition, and keystroke patterns. Bedford, Gregg, and Clinton (2009) studied the use of live-proctoring using Remote Proctor[tm]. These differing solutions for authentication controls have large variations in the strength of authentication. For example, the strength might be too strong or too weak for a given e-learning activity to secure against the threats of impersonation, which can either increase unneeded costs or impose unintended time constrains.

The understanding of fit between task and technology is important for the successful outcomes in information systems (IS) (Yu & Yu, 2010). This study highlighted the importance of fit between a suitable level of authentication strength (the technology) and e-learning activity (the task) it aims to secure against impersonation. Goodhue and Thompson (1995) defined the task-technology fit (TTF) as, "the degree to which a technology assists and individual in performing his or her portfolio of tasks" (p. 216). According to Yu and Yu (2010), "TTF is concerned with the extent to which technology

meets task-related requirements" (p. 1004). Goodhue, Klein, and March (2000) posited that the TTF seeks to predict performance and enhance the effective use of technology for given tasks.

The goal of this study was to identify suitable authentication controls based upon strength necessary for e-learning activities identified by users to have a high potential for impersonation. This study also aimed to consider the role of TTF and empirically assess if the current 'one size fits all' authentication solution in most e-learning systems is valid when it comes to securing various types of e-learning activities from impersonation fraud. This study also sought to expand the information security body of knowledge on suitable authentication controls to reduce threats of impersonation in e-learning systems, while seeking to validate the right level of authentication strength to each of the diverse activities conducted in such systems.

Problem Statement

The research problem that this study addressed is that identity and authentication controls do not reliably secure the diverse activities in Web-based systems against user impersonation fraud (Apampa et al., 2010; Flior & Kowalski, 2010; Prince, Fulton, & Garsombke, 2009). One type of Web-based system that is increasing in popularity not only in academic institutions, but also in non-academic settings is an e-learning system (González, Rodríguez, Nistal, & Rifón, 2009; Levy & Ramim, 2007). Levy and Murphy (2002) stated that an e-learning system is defined as one that:

> enables students learning via the Internet which facilitate interaction of professor-to-students, student-to-professor and students-to-students communication via

asynchronous learning tools, i.e., anytime, anywhere learning or synchronous learning tools, i.e., real-time communication, or any combination of these two, as well as, the technological, organizational and managerial infrastructure for the delivery of this service (p. 2).

In non-academic settings, e-learning systems are a strategic way for organizations from various industries to deliver training to employees in order to improve their skills or obtain certifications (Alwi & Fan, 2010; Kasraie & Kasraie, 2010). The advantages of e-learning systems are attributed to cost savings (no travel or space requirements), timeliness of information, flexibility of learning, as well as the multitude of activities to deliver content, and facilitate learning or corporate training (Park & Wentling, 2007).

Users interact with e-learning systems through a variety of learning activities. Levy (2006b) defined online learning activities in e-learning systems as, ''an educational procedure designed to stimulate learning by online experience utilizing online learning systems and tools" (p. 30). As the use of e-learning systems increases, so does the threats of IS misuse (Moini & Madni, 2009; Oakley & Singh, 2011). IS misuse is defined by D'Arcy, Hovav, and Galletta (2009) as, "a behavior that is defined by the organization as a misuse of IS resources" (p. 81-82). One of the major security challenges for e-learning systems is often attributed to the threat of IS misuse due to impersonation fraud (Apampa et al., 2010).

Apampa et al. (2010) defined impersonation fraud as "a fraudulent action with the aim of imitating a legitimate user and defrauding the security system" (p. 138). Oakley and Singh (2011) stated that fraudulent behaviors in e-learning systems potentially "undermines the value" (p. 1) of these systems. Apampa, Wills, and Argles (2011)

identified impersonation as a major threat to e-learning systems because impersonation is an intentionally act where the user collaborates with a willing participant to impersonate them. Apampa et al. (2011) identified that impersonation in the context of e-learning systems is different than those of e-banking or e-commerce systems where impersonation in these cases is unknown to the user being impersonated and typically against the users' will.

As a countermeasure to impersonation fraud, certain factors must be verified to confirm the identity of users of e-learning systems (Liou & Bhashyam, 2010). User identity is verified through the process of authentication. User identity "is a term that reflects uniqueness, sameness, and distinction" (Apampa et al., 2010, p. 136). User authentication is defined by Levy, Ramim, Furnell, and Clarke (2011) as, "the process of verifying an attempted request of an individual (i.e. 'the user') to gain access to a system" (p. 104). Authentication controls have three common factors that challenge what: a user knows (a secret), a user has (a token), or a user is (a biometric) (Flior & Kowalski, 2010; Furnell, 2007). A fourth, but less known, authentication method that Flior and Kowalski (2010) studied is continuous authentication, which is defined as, "something a user does" (p. 489). Authentication methods are technical controls used to validate a user's identity by challenging authentication factors (Flior & Kowalski, 2010; Moini & Madni, 2009). Moini and Madni (2009) examined the role of biometrics for continuous authentication of users in e-learning systems. Moini and Madni (2009) stated, "the overwhelming majority of online learning systems rely on weak authentication mechanisms to verify the remote users only at the start of the session" (p. 469). Also, they argued that authentication

strength can be increased by the number of factors challenged, however, their study was limited to an authenticating a single e-learning activity.

Flior and Kowalski (2010) stated, "each of these [authentication] methods has a number of drawbacks" (p. 488) by noting that technical controls alone are not the only security factors organizations need to consider. Furnell, Dowland, Illingworth, and Reynolds (2000) as well as Zviran and Erlich (2006) listed additional requirements to consider when selecting authentication methods such as effectiveness (strength of control such as single-factor & multi-factor), cost (value to implement), usability (friendliness or lack of interference with activity), and user acceptance (perceived attitude & usefulness toward control). A variety of authentication methods are implemented in e-learning systems to protect against impersonation fraud (González et al., 2009). Not only do authentication factors need to be verified before, but possibly throughout the duration of the e-learning activity (Calderon, Chandra, & Cheh, 2006). Rodchua, Yiadom-Boakye, and Woolsey (2001) studied the use of live proctoring along with biometric authentication as a means to verify identity users in e-learning systems. Their study was limited to authenticating only a single e-learning activity. Inaba, Watanabe, and Kodate (2003) as well as Penteado and Marana (2009) studied face recognition as a means to continuously authenticate users in e-learning systems. Their studies were limited to authenticating the e-learning system but did not include the suitability assessment for diverse e-learning activities.

According to Alwi and Fan (2010), much of the research on impersonation fraud has been focused toward improving authentication methods from a technical perspective. Authentication methods have been shown to be effective technical deterrents to IS

misuse, however, the human element cannot be ignored (Vroom & Von Solms, 2004). Apampa et al. (2010) indicated that users are a valuable asset to e-learning systems. Levy, Ramim, and Hackney (2013) investigated user perceptions toward ethical severity on five types of security attacks, including impersonation, and indicated that majority of users (90% out of a sample of 519) are "ethically driven" (p. 78). King, Guyette, and Piotrowski (2009) found that more than 70% out of a sample of 121 users held the perception that their peers participated in fraudulent behaviors in e-learning systems. King et al. (2009) studied views toward misconduct in e-assessments and stated that "contemporary students have rather lax attitudes toward suspect behaviors or ethical issues" (p. 7). However, their study only measured business student's views as opposed to a more diverse sampling of the university's entire student population. This type of selective sampling may question external validity by producing a systematic effect leading to a reduction of individual differences within responses (Straub, 1989).

Prince et al. (2009) identified an increase in user perception of the threats of impersonation fraud in e-learning systems. Bailie and Jortberg (2009) identified the importance of student perceptions and measured satisfaction of identity testing within e-learning systems. However, Prince et al. (2009) as well as Bailie and Jortberg (2009) only measured user perceptions toward a single authentication method to access a single type of e-learning activity. Oakley and Singh (2011) explored the formal and informal constructs of the technical, formal, and informal (TFI) framework in order to "develop normative guidance that can lead to more effective security control in e-learning" (p. 2). However, the Oakley and Singh (2011) study did not explore the technical construct, which organizations need to give equal consideration in order to effectively minimize IS

misuse (Dhillon, 1999). Thus, it appeared that additional research on the specific authentication methods to reduce the threats of impersonation fraud for multiple activities within e-learning systems was warranted.

Simon and Chaney (2006) as well as Peslak (2008) posited gender differences are significant when considering unethical behaviors such as accessing unauthorized files. Additionally, Peslak (2008) further indicated that increasing age leads to more experience in terms of system usage, which is a significant indicator towards ethical behavior. Lanier (2006) as well as Gibson, Khey, and Schreck (2008) supported that demographic variables such as age and gender are significant to predict user's intent to misuse e-learning systems. Gibson et al. (2008) indicated that males and younger users were more likely to engage in unethical conduct than females and older users, respectively. Thus, it appears that demographic variables were significant when it came to the research of suitability of authentication methods for e-learning activities.

Helkala and Snekkenes (2009) suggested the need for research to customize the selection of suitable authentication controls in terms of cost and usability for each usage scenario. Goodhue and Thompson (1995) recognized that the linkage between the technology an individual used and the types of tasks it supported has an impact on IS success. Dishaw and Strong (1999) further supported that "systems implementation research notes the need for fit between tasks, technologies, and users" (p.12). Goodhue (1998) suggested that in IS, the technology required by users for a given task serves as a basis for the task-technology fit. However, the study was limited to only one task involving managerial decision making within an IS.

Knowledge about authentication methods for diverse activities in e-learning systems appeared to be significant. Additionally, knowledge about the threats of impersonation and the complimenting multi-factor authentication methods for diverse activities in e-learning systems, as opposed to single sign-on upon entry or just a strong authentication in a single activity, appeared to be significant, which warranted additional work. Moreover, additional research can provide a guide to help e-learning system developers and providers realize what activities they should or should not invest in establishing more robust authentications.

Dissertation Goals

The main goal of this research study was to empirically assess what *authentication methods* and *strength* users perceived to be most suitable for activities in e-learning systems based on the threats of impersonation. The need for this work was demonstrated by the work of Levy and Ramim (2007) who stated that "future research may be fruitful by examining students' attitudes and psychological aspects associated with the proposed solution of e-exam user's authentication" (p. 99). Additional, Levy et al. (2011) who stated that "developing a single approach to address proper authentication of e-learners throughout all their e-learning activities appears to pose a challenge" (p. 103), identified the need to use suitable authentication methods for the diverse activities in e-learning systems.

This study was built upon previous research by Apampa et al. (2010) that identified impersonation fraud as a major threat to summative e-assessments. Summative e-assessments are defined as high-stake examinations while formative e-assessments are

enrichment activities in e-learning systems to advance learning (Apampa et al., 2010). This study also built upon the work of Levy (2006b) that identified the top 10 most valuable activities in e-learning systems, and the work of Levy (2008) that developed critical value factors (CVF) for activities in e-learning systems. These CVF organize the top activities in e-learning systems into five categories: (a) Collaborative, Social, and Passive Learning Activities; (b) Formal Communication Activities; (c) Formal Learning Activities; (d) Logistic Activities; and (e) Printing Activities. This research study used summative and formal learning activities within these categories to identify the activities that users perceived to have a high potential for impersonation fraud. This study also built upon Oakley and Singh (2011), which focused on the socio-technical aspects of e-learning security in order to build a more holistic view of the system. Additionally, this study was built upon the study by Moini and Madni (2009), which proposed that current weak authentication methods are not suitable to defend against user impersonation. Finally, this study was built upon the theoretical foundations of TTF, which proposed the need for both task and technology to fit in order to achieve the expected outcome within the use of IS (Goodhue & Thompson, 1995). Thus, this research study reported on the assessment of what levels of authentication strength users perceived suitable in addressing impersonation fraud for assessed e-learning activities.

The first specific goal of this study sought to determine what e-learning activities are perceived by users to have a high potential for threats of impersonation (1a) and what e-learning activities user perceived that their peers will identify to have a high potential for threats of impersonation (1b). After the first (1a) and second (1b) parts of the first specific goal were identified, this specific goal sought to determine if there are significant

differences for the e-learning activities perceived by users to have a high potential for impersonation than what users perceived that their peers will identify (1c).

The second specific goal of this study sought to determine what levels of authentication strength are perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities (2a) and what levels of authentication strength are perceived by users that their peers will identify to be most suitable against the threats of impersonation for these assessed e-learning activities (2b). After the first (2a) and second (2b) parts of the second specific goal were identified, this specific goal sought to determine if there are significant differences on the levels of authentication strength that are perceived to be most suitable against the threats of impersonation for these assessed e-learning activities between users and those perceived by users that their peers will identify (2c).

The third specific goal of this study sought to assess the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities (3a) and the significant components of the levels of authentication strength perceived by users that their peers will identify to be most suitable against the threats of impersonation for these assessed e-learning activities (3b). After the first (3a) and second (3b) parts of this third specific goal were identified, this specific goal sought to identify the differences between the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities versus those perceived by users that their peers will identify (3c). The fourth specific goal of this study was to measure if there were significant differences of perception of high

potential for threats of impersonation based on gender (4a), age (4b), and e-learning experience (4c).

Research Questions

Research on impersonation fraud is primarily from the perspective of technical authentication access controls and a limited amount is from the perception of users of the system. In addition, research studies refer to summative exams as the only activity in e-learning systems being threatened by impersonation (Apampa et al., 2010; King et al., 2009; Prince et al., 2009). Given than, e-learning systems have a number of activities that are susceptible to impersonation, which contribute to the value of the system, additional e-learning activities that warranted mitigation needed to be studied (Levy, 2006b). Additionally, a limited number of research studies have been conducted to measure the user's perception of suitable authentication methods and levels of authentication strength to reduce impersonation fraud. Bedford et al. (2009) investigated student acceptance of a deterrence technology called Remote Proctor[tm]. Bedford et al. (2009) used perceived usefulness and perceived ease of use based upon the work of Davis (1989) to measure the user's perception of strength of authentication to reduce misconduct in e-assessments. Although Bedford et al. (2009) did measure user's perception, only the use of live-proctor authentication on a single activity in e-learning systems was used by experienced computer users.

Knowledge of impersonation and suitable authentication methods to reduce the threats of impersonation has implications in a multitude of industries such as e-banking. Howell and Wei (2010) stated that "banks that have not yet addressed the need for multi-factor

authentication should have that at the top of their [Information Technology] IT priority list" (p. 73). Given this demonstrated need for additional research related to authentication methods in e-learning systems the research questions of this study were:

RQ1a: What e-learning activities are perceived by users to have a high potential for threats of impersonation?

RQ1b: What e-learning activities users perceived that their peers will identify to have a high potential for threats of impersonation?

RQ1c: How do the e-learning activities perceived by users to have a high potential for impersonation differ than what is perceived by users that their peers will identify?

RQ2a: What levels of authentication strength are perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities?

RQ2b: What levels of authentication strength are perceived by users that their peers will identify to be most suitable against the threats of impersonation for these assessed e-learning activities?

RQ2c: How do the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities differ than what is perceived by users that their peers will identify?

RQ3a: What are the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities?

RQ3b: What are the significant components of the levels of authentication strength

perceived by users that their peers will identify to be most suitable against the

threats of impersonation for these assessed e-learning activities?

RQ3c: What are the differences between the significant components of the levels of

authentication strength perceived by users to be most suitable against the threats

of impersonation for these assessed e-learning activities versus than what is

perceived by users that their peers will identify?

RQ4a: Are there significant differences of perception of high potential for threats of

impersonation based on gender?

RQ4b: Are there significant differences of perception of high potential for threats of

impersonation based on age?

RQ4c: Are there significant differences of perception of high potential for threats of

impersonation based on e-learning experience?

Figures 1 and 2 depict an example of how RQ1a and RQ1b as well as RQ2a and RQ2b

will assess e-learning activities for high potential for impersonation and suitable

authentication strength.

Figure 1. Research Factorial Design for Assessment of E-learning Activities and Suitable Authentication Strength (RQ1s & RQ2s)
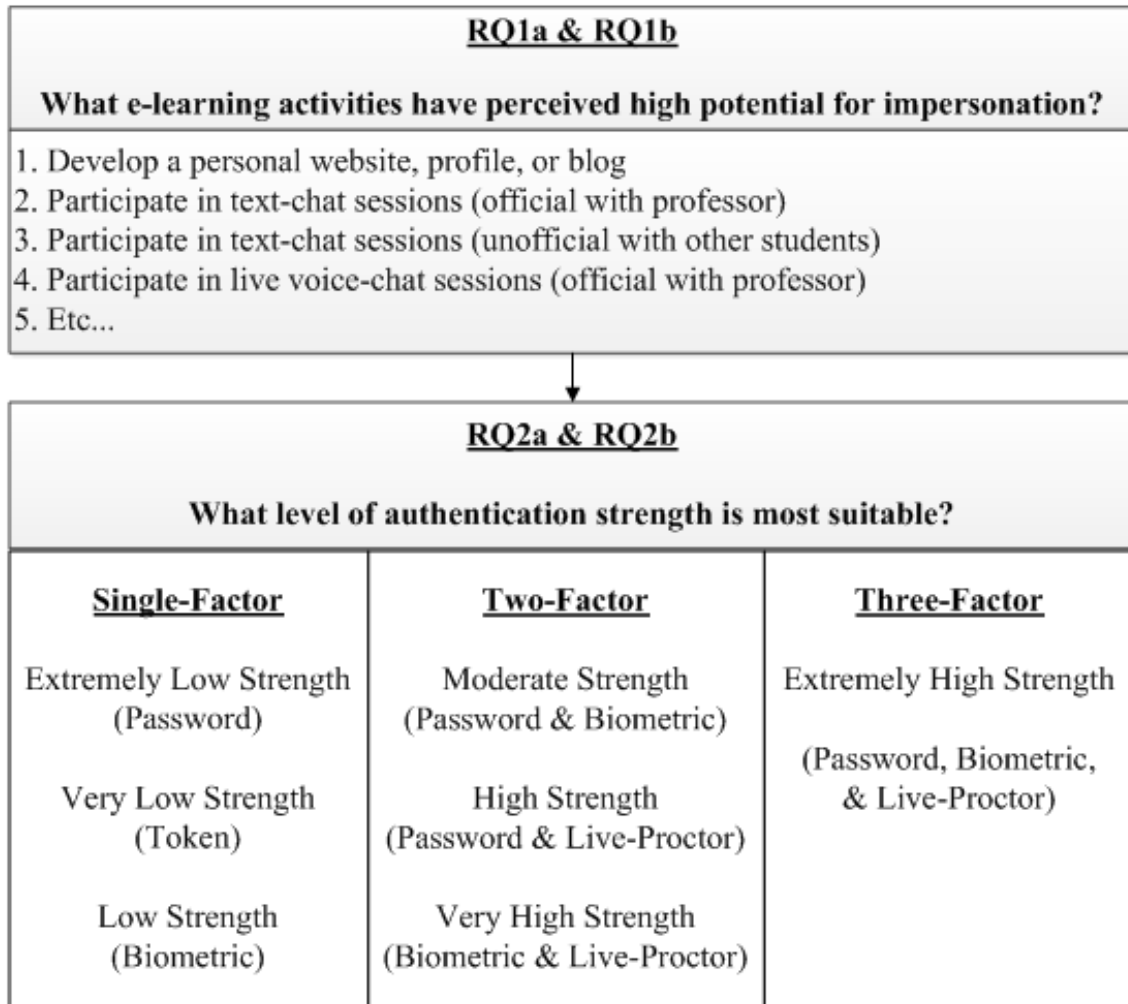
Figure 2. Process of Assessment for E-Learning Activities and
Suitable Authentication Strength

The same e-learning activities that were assessed for high potential of impersonation were used in RQ2a and RQ2b, respectively. RQ2a and RQ2b identified what levels of authentication strength to be most suitable for assessed e-learning activities. Figure 3 illustrates images of examples for the four types of levels of authentication strength varying from extremely low strength, very low strength, or low strength (single-factor), onto moderate strength, high strength, or very high strength (two-factor), and upward to extremely high strength (three-factor).

Figure 3. Types of Levels for Authentication Strength:
Username/Password, Token, Biometric Finger Scanning, and Live-Proctor[tm]

Relevance and Significance

Relevance

D'Arcy et al. (2009) identified the need for authentication controls to reduce the significant threat to organizations from the intentional IS misuse of systems by internal users. Marais, Argles, and Von Solms (2006) asserted that although e-learning system security is a well investigated area, the research has not significantly fulfilled the need to secure e-learning activities. Apampa et al. (2010) as well as Galanxhi and Nah (2007) claimed that current authentication controls are insufficient to secure against user impersonation within Web-based systems and can threaten the integrity of the system. To support the significance of this issue, Oakley and Singh (2011) noted that it is critical for e-learning providers to maintain the effectiveness of the system by improving user authentication to reduce IS misuse. Levy and Ramim (2007) provided further relevance to this issue by proposing biometric solutions to authenticate users to reduce the threats of impersonation throughout the activity session, however, did not empirically test it.

The purpose of this study was to extend and integrate current research on authentication strengths and e-learning activities in Web-based systems. Alwi and Fan (2010) posited that single-factor authentication such as passwords or even multi-factor authentication, which combines at least two factors, does not protect an e-learning

activity from impersonation threats when initiated solely upon entry. Apampa et al. (2010) proposed a user security model aimed to reduce impersonation threats by using stronger multi-biometric authentication controls for assessed e-learning activities. Levy et al. (2011) supported the need for stronger authentication in their study, which measured user acceptance to provide biometric data in an e-learning environment. They claimed that e-learning providers have "the challenge to properly authenticate learners who are engaged in various e-learning activities is still compelling" (Levy et al., 2011, p. 109).

Significance

The significance of this study was to identify what levels of authentication strength are perceived by users as suitable for e-learning activities with high potential for impersonation. Currently, there are no known 'best practices' when it comes to authenticating users in e-learning activities. Levy et al. (2011) identified this significance by implicating the need to improve authentication for various e-learning activities. Implementing authentication controls without properly matching suitable authentication controls to e-learning activities does not sufficiently reduce IS misuse (Alwi & Fan, 2010). The significance of this study also expanded the literature on suitable authentication controls necessary for various e-learning activities not only in academic environments but also in non-academic industries such e-banking, which has seen an increase in federal mandates to reduce a 'one size fits all' approach to authentication (Levy et al., 2011; Yang & Padmanabhan, 2010). Although there have been numerous authentication methods proposed in e-learning, further research into suitable authentication for e-learning activities is still relevant and significant to improve IS security (Levy & Ramim, 2007).

Barriers and Issues

There were a few known barriers and issues with conducting this exploratory study. One barrier of this study was to identify which e-learning activities to select for measurement. There are numerous studies that identified key activities in e-learning systems (Adams, 2012; Bailie & Jortberg, 2009; Levy, 2006b). In order to mitigate this barrier, this study built upon those studies and compiled a list of top e-learning activities. An expert panel reviewed the e-learning activities that formed that basis for this study and modifications were made as necessary.

A second barrier was the participants in the survey must have been familiar with the e-learning activities being measured and have had experience with the e-learning process, therefore, the survey was only distributed to active e-learning participants. Similarly, the third barrier depends on participants having knowledge about the authentication methods being measured to reduce threats of impersonation. To address this barrier, a detailed definition describing each authentication control along with images to illustrate examples of username/password, tokens, biometrics, and live-proctor authentication was described within the survey.

An issue for this study was that the survey asked for participants to self-report their perceptions. Therefore, the reliability of the data collected was dependent on the participants' honestly of their responses. Because it is difficult to measure IS misuse when self-reported as it is often under-reported by users (Gibson et al., 2008), this study measured user reported perceptions of what level of misuse they think occurs for each e-learning activity. Although researchers such as Gupta, Cunningham, and Arya (2009) warned that actual behavior does not always relate to perceived behavior, a number of

studies relating to academia have used anonymous surveys to determine perceived misuse (D'Arcy et al., 2009; Hollinger & Lanza-Kaduce, 2009). Additionally, DeLone and McLean (1992) indicated that studies in IS measuring perception of performance are often used as surrogates of actual performance.

A final barrier for this study was due to the fact that a link to the Web-based survey was distributed via email, the response rate was highly dependent on recipients taking the time to read and voluntarily participate in the survey with no incentives. Stanton and Rogelberg (2001) recommended strategies to increase response rates such as sending out an advance notice prior to e-mailing the survey and offering the recipients an opportunity to decline participation in the study. Thus, to mitigate such barrier, this study followed the recommendations made by Stanton and Rogelberg (2001).

Assumptions, Limitations, and Delimitations

Assumptions

Leedy and Ormrod (2010) stated that "assumptions are so basic that, without them, the research problem itself could not exist" (p. 59). An assumption for this study was that since the survey results contained no identifiable information regarding the respondents, participants answered truthfully to the best of their knowledge. However, because the study surveys perceptions of potential IS misuse, Hollinger and Lanza-Kaduce (2009) suggested that anonymous surveys are the best method to obtain such data. Another assumption is that since the population included only e-learners, respondents had experience with the e-learning activities used within the survey.

Limitations

A limitation of this study was that not all respondents had experience with each authentication control that was discussed in the survey. This limitation was moderated by providing both a description and image to demonstrate types of levels for authentication strength commonly used in Web-based systems to authenticate users. Moreover, given the speed at which technology is changing, it is probably also feasible that a majority of the participants did have experience with several of the authentication controls surveyed. Another limitation was that the e-learning activities used in this study were selected from those identified as the most valuable used within e-learning systems in academic environments. Although the environment may be a factor, the generalizability to e-learning systems in non-academic results should not be affected.

Delimitations

A primary delimitation for this study was that it was confined to the risk of impersonation and the authentication factors that are most suitable to reduce that risk. This study did not extend into other types of risk that have been prevalent in e-learning systems. Additionally, this study was not aimed to research motivational behaviors for why users choose to deliberately impersonate. Another delimitation for this study was the population included only respondents who have used e-learning systems and not users of other types of Web-based systems such as e-banking, e-government, or e-medicine, to name a few.

Definition of Terms

The following section provides the terms and definitions used in this research.

Activity – "systems of collaborative human practice and generator of a constantly and continuously emerging context" (Levy, 2008, p. 1665).

Analysis of Covariance (ANCOVA) – "adjusts the effects of variables that are related to the dependent variables" (Mertler & Vannatta, 2010, p.93).

Authentication control – preventative layer tools to protect against IS misuse (Straub & Nance, 1990).

Authentication method – technical controls used to validate a user's identity by challenging authentication factors (Flior & Kowalski, 2010; Moini & Madni, 2009).

Authentication strength – measured by the number of authentication factors used to identify a remote system user (Asha & Chellappan, 2008).

Biometrics – the identification of an individual based on physiological and behavioral characteristics (Gao, 2012).

Continuous authentication – "something a user does" (Flior & Kowalski, 2010, p. 489).

Control – "the use of interventions by a controller to promote a preferred behavior of a system being controlled" (Van Aken, 1978, p. 44).

Critical value factors – "the factors that educational institutions should pay attention to in order to increase the learners' perceived value, which in turn may help reduce dropout in online learner courses" (Levy, 2008, p. 1664).

Cronbach's Alpha – "a reliability coefficient that indicates how well that items in a set are positively correlated to one another" (Sekaran, 2003, p. 307).

E-assessments – "the end-to-end electronic assessment processes where ICT is used for the presentation of assessment activity and the recording of responses" (JISC, 2006, p. 45).

E-learning – the learning process over the Internet through the use of computers and networks (Moini & Madni, 2009).

E-learning system – delivers learning in an instructional context via the Internet using technical tools (Welsh, Wanberg, Brown, & Simmering, 2003).

Formative e-assessments – enrichment activities in e-learning systems to advance learning (Apampa et al., 2010).

Impersonation fraud – "a fraudulent action with the aim of imitating a legitimate user and defrauding the security system" (Apampa et al., 2010, p. 138).

IS misuse – "an individual's intention to perform a behavior that is defined by the organization as a misuse of resources" (D'Arcy et al., 2009, p. 81-82).

Live-proctor authentication – observation of remote e-learners via a Web-cam and a live proctor over the internet, irrespective of the location (Kitahara, Westfall, & Mankelwicz, 2011).

Online learning activity – "as an educational procedure designed to stimulate learning by online experience utilizing online learning systems and tools" (Levy, 2006b, p. 30).

Outlier – "cases with unusual or extreme values at one or both ends of a sample distribution" (Mertler & Vannatta, 2010, p.27).

Pre-Analysis Data Screening – "pre-analysis data preparation deals with the process of detecting irregularities or problems with the collected data" (Levy, 2006, p. 150).

Suitable authentication – "an authentication product must comply with usage and environment-related requirements dictated by the scenario" (Helkala & Snekkenes, p. 4).

Summative e-assessments – high-stake examinations in e-learning systems (Apampa et al., 2010).

Task-Technology Fit – "concerned with the extent to which technology meets task-related requirements." (Yu & Yu, 2010, p. 1004).

Token – stored information about one or more authentication methods such as username/password or biometric identifiers (Bolle, Connell, Pankanti, Ratha, & Senior, 2003).

User authentication – "the process of verifying an attempted request of an individual (i.e. 'the user') to gain access to a system" (Levy et al., 2011, p. 104).

User identity – is a term that reflects uniqueness, sameness, and distinction" (Apampa et al., 2010, p. 136).

Summary

Chapter one provides the background and the problem statement for the research problem studied, which is securing Web-based systems against impersonation and the identification of suitable authentication controls for e-learning activities with high potential of impersonation (Apampa, et al., 2010; Helkala & Snekkenes, 2009). This research expanded the literature on the risk of impersonation for top e-learning activities (Aceves & Aceves, 2009; Flior & Kowalski, 2010; Oakley & Singh, 2011; Prince et al., 2009). This research also expanded the literature on the suitable types of authentication controls using the theory of TTF (Flior & Kowalski, 2010; Furnell, 2007; Goodhue, 1998; Helkala & Snekkenes, 2009).

The main goal of this research was to empirically assess what *authentication methods* and *strength* users perceived to be most suitable for activities in e-learning systems based on the threats of impersonation. Four specific goals were stated. First, to seek to determine what e-learning activities were perceived by users and perceived by users that their peers will identify to have a high potential for threats of impersonation; second, to seek to determine what levels of authentication strength were perceived by users and perceived by users that their peers will identify to be most suitable against the threats of impersonation for these assessed e-learning activities; third, to assess the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities; finally, fourth to measure if there were significant differences of perception of high potential for threats of impersonation based on gender, age, and e-learning experience.

The relevance and significance section discussed how this study extended the current literature on authentication and e-learning systems by integrating the research in e-learning activities and authentication to identify suitable levels of authentication strength for diverse e-learning activities. Barriers and issues section outlined the challenges this study faced throughout the research process. Barriers to this research goal were identified as developing a valid set of e-learning activities, the study of perceived behavior in lieu of actual behavior, and response rates. This research used previous studies to compile top valuable e-learning activities in e-learning systems (Adams, 2012; Bailie & Jortberg, 2009; Levy, 2006b). This research also used an anonymous survey to reduce the risk of under-reported IS misuse (Gupta et al., 2009). Finally a participation letter was sent along with the link to the Web-based survey to increase response rates

(Stanton & Rogelberg, 2001). Assumptions, limitations, and delimitations identified factors that were improvable, out of control of study, or constrained by the approach, respectively. Assumptions such as prior knowledge of e-learning activities used in Web-based systems and truthful responses were identified. Limitations included knowledge of the authentication controls used and generalizability to other e-learning environments. Delimitations were to the population of experience e-learners and the focus on only impersonation fraud.

The remainder of this dissertation study is organized as the following. Chapter two expands the body of knowledge through a literature review pertaining to Web-based systems, e-learning systems, Activity Theory, e-learning activities, impersonation fraud, authentication, and TTF. Chapter three details the research design in terms of methodology, data gathering, and analysis. Chapter four details the three phases of this study including development and validation of the survey instrument and data analysis of data gathered. Chapter five discusses the conclusions of the study along with implications and recommendations for future research. Finally, references and the appendices, which include the survey instrument, participation letter, and IRB approval are the last sections of this dissertation study.

Chapter 2

Review of the Literature

Introduction

This literature review provides the research background on Web-based systems, e-learning systems, Activity Theory, e-learning activities, impersonation fraud, authentication, and TTF. In order to integrate the body of knowledge, the context of this review is specific to e-learning systems. The purpose of this literature review is to develop relevant support for an exploratory study on suitable authentication controls for e-learning activities to protect against impersonation. Finally, there is a section on what is known and unknown that identifies the gap in the literature as a framework for the unique contribution of this study.

Web-based Systems

Organizations have been concerned about securing IS as long as businesses have been using computer systems (Lee & Lee, 2002). IS security is concerned with protecting system assets from threats in order to align with organizational goals (Straub & Nance, 1990). Knowledge on how to sufficiently secure business transactions is currently still one of the main problems organizations face in IS (Fenz & Ekelhart, 2009). In the past two decades, the use of the Internet for the implementation of Web-based systems has been expanding in a multitude of industries such as e-banking, e-government, and

e-learning ('e' refers to electronic), which have the common characteristic of providing

e-services to their users (Alwi & Fan, 2010).

In meeting with new competitive strategies, banking institutions offer convenient

e-banking services to consumers through a number of online activities such as banking

support, account inquiries, payment services, and mobile banking (Howell & Wei, 2010).

Web-based systems have enabled the use of e-government to improve transparency and

grant access to information at federal, state, and local levels through the use of activities

such as online application submission, employee inquiries, and tax services (Cuillier &

Piotrowski, 2009). Bertot, Jaeger, and Grimes (2010) defined transparency as, "essential

to democratic participation, trust in government, prevention of corruption, informed

decision-making, accuracy of government information, and provision of information to

the public, companies, and journalist, among other essential functions in society" (p.

264). E-learning systems are becoming one of the largest growing sectors of Web-based

systems (Alwi & Fan, 2010). This growth is fueled by the need for organizations to

provide a more flexible, cost-efficient approach to learning than can be offered via

traditional face-to-face classrooms (Park & Wentling, 2007). These studies demonstrate

that the growth of Web-based systems to deliver e-services is prevalent across all

industries. Table 1 lists a summary of research studies regarding the growing use of

various types of Web-based systems and technologies issues on securing those systems.

Table 1. Summary of Research Studies on Web-based Systems

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Alwi & Fan, 2010	Theoretical	Commentary	Discussion on Web-based systems definitions, characteristics, & growth	E-learning institutions need a security management framework to serve as a guide for securing Web-based systems.
Bertot et al., 2010	Theoretical	Commentary	Discussion on attitudes toward transparency in Web-based systems	Implementing Web-based system technologies for e-government is challenging. Review of technology requirements lead to long-term success.
Cuillier & Piotrowski, 2009	Meta-analysis	3 studies (1: online students, 2: national online survey, 3: US phone survey)	Case study measuring motivation & gratification toward uses of Web-based systems	Reliance on Web-based systems is increasing in e-government.
Fenz & Ekelhart, 2009	Exploratory	Best-practice guidelines used in security ontology models	Threats & vulnerabilities for Web-based systems	A lack of knowledge about risks is one reason for inadequate information security.
Howell & Wei, 2010	Empirical	20 banks Websites	Case study measuring CVF for implementing Web-based systems	Securing Web-based e-banking activities has not been addressed by institutions effectively.

Table 1. Summary of Research Studies on Web-based Systems (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Lee & Lee, 2002	Meta-analysis	Social criminology theories	Proposed a new IS misuse model	Misconduct is influenced by both social and technical factors.
Park & Wentling, 2007	Empirical	47 Web-based learners	Web-based survey measuring attitudes & perceived usability of Web-based systems	Users' attitudes significantly influence perceived usability of Web-based systems.
Straub & Nance, 1990	Empirical	1063 computer abuse victims	Survey measuring IS misuse detection methods	50% of misuse incidents were detected with normal system controls and 16% with purposeful investigations. A high level of visible detection methods is desirable to defer deliberate misuse.

E-learning Systems

An e-learning system is considered a subset of Web-based systems that can include

distance learning (online only), blended learning (distance learning & face-to-face), or

self-paced learning (Alwi & Fan, 2010). An e-learning system delivers learning in an

instructional context via the Internet using technical tools (Welsh et al., 2003). The use of

an e-learning system serves as a special type of IS where the system is used to conduct

learning activities (Wang, Wang, & Shee, 2007). The global market for the use of e-

learning systems is predicted to reach nearly $50 billion by 2014 (Eom, Ashill, Arbaugh,

& Stapleton, 2012). Because of its flexibility to provide cost-effective learning without the limitations of time and location, e-learning systems have been embraced by both academic as well as non-academic markets (Gunasekaran, McNeil, & Shaul, 2002).

Research on e-learning systems in the IS literature has primarily been from the perspective of IS success, which focuses mainly on system quality (Eom et al., 2012; Wang et al., 2005). There is a need for research to shift focus from e-learning system success to human factors (Eom et al., 2012). For example, a critical issue that needs further research is the challenge to control the use of activities within the e-learning system from IS misuse from impersonation fraud (Bailie & Jortberg, 2009). Although, the Higher Learning Commission (HLC) created a policy that requires an organization to implement a process in order to ensure the authentication of users within an e-learning system, as the use of e-learning systems grow, so will the need for stronger authentication (Bailie & Jortberg, 2009).

Non-academic Uses of E-learning Systems

Employees are in constant need to improve their knowledge and skills for the workplace (Roy & Raymond, 2008). In order to maintain a competitive edge, organizations have adopted e-learning as a venue for workers to stay up-to-date with training requirements (Cheng, Wang, Yang, & Peng, 2011; Wang et al., 2007). The benefits of using e-learning systems within organizations are attributed to reduced expenses for travel, the ability to maintain current learning materials, and the minimized disruption to workplace production that traditional classroom training often requires (Berge & Giles, 2008). Ultimately, the goal of e-learning within these non-academic

environments is to improve job performance, increase business results, and bring about positive changes within the organization (Cheng et al., 2011).

In order to meet job-specific competencies, organizations employ e-learning activities such as learning modules, discussions, and exams for employees to complete training requirements (Bondarouk & Ruël, 2010). The investment in e-learning is substantial as evident by the e-learning survey reported by the American Society for Training and Development (ASTD) where 100% of the 348 responding organizations claimed to allocate some portion of the training budget for e-learning (Green & McGill, 2011). This is an increase compared to ASTD's same survey in 2004, where only 38% of 246 respondents indicated that there was some type of training being delivered via e-learning (Suqrue & Rivera, 2005). As early as 2000, the estimated expenditures for e-learning exceeded $2 trillion worldwide (Fry, 2001). These results highlight the adoption of e-learning systems within organizations as a means to provide valuable, continuous training, and knowledge to employees.

Academic uses of e-learning systems

Due to technical advances, e-learning systems have allowed universities to provide learning through a wide breadth of learning activities to students without geographic limitations (Lanier, 2006). To remain competitive, universities across the globe have integrated e-learning into their programs (Moini & Madni, 2009; Prince et al., 2009; Selim, 2007). American universities have already enrolled well over a million e-learning students from over 50,000 course offerings (Lawrence, 2003). Ossiannilsson and Landgren, (2012) stated in their study that "during the last 10 years, the European Commission has worked strategically with several initiatives and white papers to

develop, enhance, and implement e-learning" (p. 43). Budget constrained universities are shifting investing budgets toward e-learning programs as opposed to enlarging campuses (Lanier, 2006).

For students, e-learning offers a flexible, cost saving alternative to traditional classroom learning (Alwi & Fan, 2010). Students can save time on travel, money on printing, and increase access to learning materials (Park & Wentling, 2007). E-learning offers a wide variety of learning activities such as assignments, assessments, discussion posts, team based projects, live chat sessions, and access to learning materials to encourage interaction among users (Levy, 2006a). There have been studies aimed to recognize the top activities users find integral and most valuable within e-learning systems (Bailie & Jortberg, 2009; Levy, 2006a; Levy, 2006b). In order to select the most valuable activities in e-learning for assessment in this study, activity theory was used as a lens to discuss how activities, people, and systems interact to reach a common outcome. Table 2 lists a summary of studies specifically for e-learning systems and relevant literature related to success factors for their implementation.

Table 2. Summary of Research Studies on E-learning Systems

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Alwi & Fan, 2010	Theoretical	Commentary	Discussion on e-learning definitions, characteristics, & growth	E-learning institutions need a security management framework to serve as a guide for securing Web-based systems.

Table 2. Summary of Research Studies on E-learning Systems (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Bailie & Jortberg, 2009	Empirical	183 online users	Case study measuring identity verification success in e-learning systems	92% passed user identification test at the system level. Further research is necessary for stronger authentication for specific activities.
Berge & Giles, 2008	Theoretical	Commentary	Discussion on strategic planning for implementing e-learning system framework	Warned that failure to establish a technology infrastructure for all activities is crippling for e-learning.
Cheng et al., 2011	Experiment	222 employees	Survey measuring perceived individual learning support, perceived support for enhancing social ties, perceived support for promoting a norm of cooperation, & intention to use e-learning systems.	E-learning systems with advanced technologies used in the workplace are widely adopted with success in organizational settings.

Table 2. Summary of Research Studies on E-learning Systems (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Eom et al., 2012	Empirical	674 online under-graduate and graduate students	Survey measuring system use & system quality as critical success factors in e-learning systems	No significant relationship exists between system use and system quality in e-learning systems due to the mandatory participation. E-learning systems research should focus critical success factors based upon e-learning outcomes.
Fry, 2001	Theoretical	Commentary	E-learning system success factors	Technologies used in e-learning are crucial for effectiveness and needs to be addressed.
Green & McGill, 2011	Empirical	348 organizations	Survey measuring adoption rates of e-learning systems	100% claimed to allocate a budget for e-learning.
Gunasekaran et al., 2002	Theoretical	Literature review	Discussion on critical success factors in e-learning systems.	E-learning is relevant in all business sectors.
Ossiannilsson & Landgren, 2012	Exploratory	8 universities	Case study creating a framework for critical success in e-learning systems	Most studies on e-learning systems have not focused on the technical factors to meet the needs of the organization.

Table 2. Summary of Research Studies on E-learning Systems (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Park & Wentling, 2007	Empirical	47 employees	Web-based survey measuring perceived usability & satisfaction of e-learning systems	Users' attitudes significantly influence perceived usability of e-learning systems.
Roy & Raymond, 2008	Exploratory	16 e-learning organizations	Case study measuring awareness, use, & perceived benefits of e-learning systems	More support is required for managers to efficiently and effectively implement appropriate e-learning technologies.
Selim, 2007	Empirical	538 under-graduate students	Survey measuring: attitude towards & control of the technology, computer competency, interactive collaboration, e-learning course content, ease of access, infrastructure, & support as success factors for e-learning systems	Technology factors are significant for measuring system success among users.

Table 2. Summary of Research Studies on E-learning Systems (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Wang et al., 2007	Empirical	206 e-learners	Survey measuring perceived overall performance and perceived overall success of e-learning systems	There is a need to extend the traditional IS success models include e-learning systems.
Welsh et al., 2003	Theoretical	Literature review	Discussion on drawbacks on e-learning systems.	Institutions must carefully consider the technology infrastructure carefully when in order to successfully implement e-learning systems.

Activity Theory

Activity theory dates back to the 1920s when a group of Russian psychologists

developed a set of principles to explain the relationship between humans and artifacts in

social environments (Levy, 2008). Activity theory has evolved over three generations of

research (Engeström, 2001). From a philosophical perspective, Levy (2008) defined an

activity as, "systems of collaborative human practice and sees it as the generator of a

constantly and continuously emerging context" (p. 1665). Using a systems perspective,

Frederickson, Reed, and Clifford (2005) defined an activity as, "a form of doing by a

subject directed at an object using tools in order to transform it into an outcome" (p. 660).

Building on these definitions, in IS, activity theory is considered a socio-cultural theory

involving complex relationships that focuses on how people work collaboratively using

learning objects within a common community (Liu & Schwen, 2006). Engeström (2001)

created an activity system model, shown in Figure 4, where subjects (people) work within

a community toward a common outcome. In activity theory, the community is mediated

by instruments, rules, and the division of labor. All the components (subjects, objects, &

community) of the model work collaboratively to achieve an outcome.
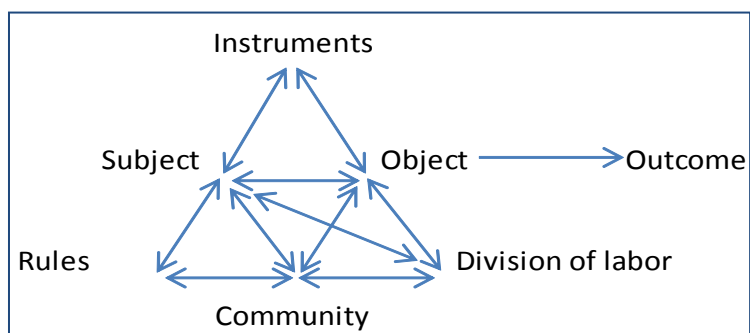
Figure 4. Activity System Model (Engeström, 2001)

Lastly, Hasan and Crawford (2003) viewed Activity Theory from a cultural-historical

perspective, depicted in the model in Figure 5, where people (subjects) engage in actions

and operations (activities) with a common purpose (object), mediated by tools to reach an

explicit outcome.
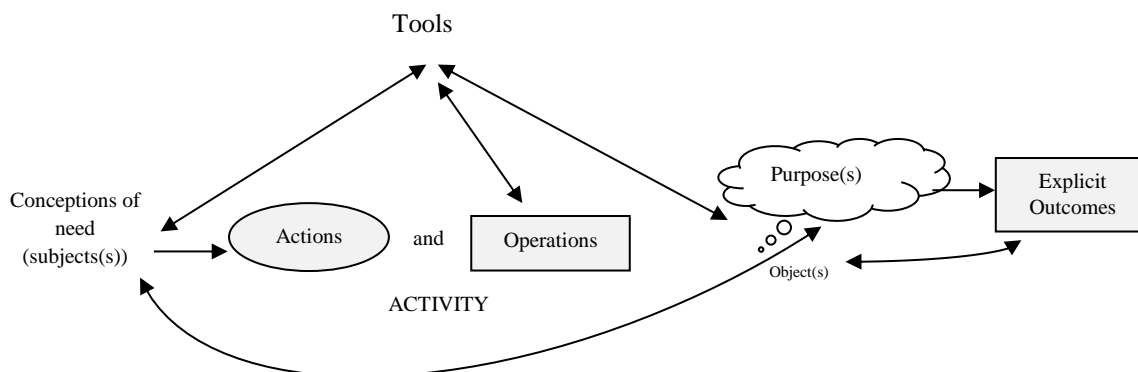
Figure 5. Activity Theory in Context of Cultural-Historical Activity Theory
(Hasan & Crawford, 2003)

Walker (2004) studied Activity Theory in the context of online learning in order to understand Web-based systems. Crawford (2001) summarized Activity Theory in the context of learning as, "the development of a learner's framework of knowledge and understanding through the interactive activities that occur within a learning situation" (p. 69). For the purpose of this study, another variation of Activity Theory developed by Levy (2006b) is applied as a theoretical framework. Grounded in Activity Theory, Levy (2006b) modified the conceptual map in context of online learning activities (e-learning activities) shown in Figure 6.
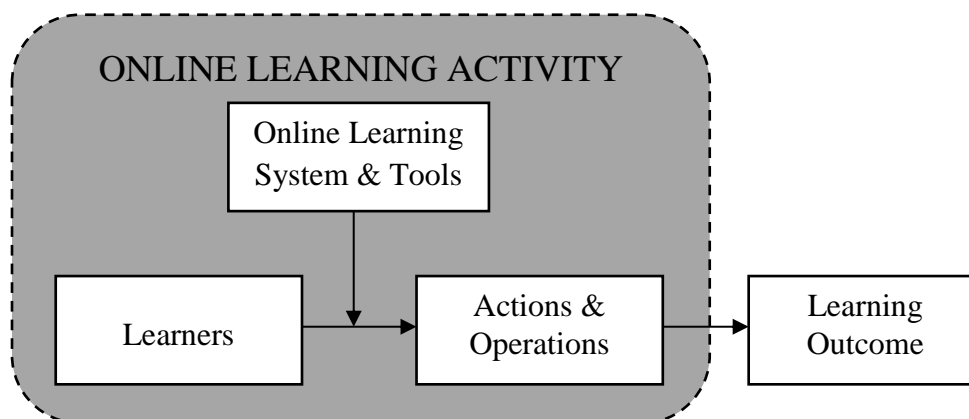
Figure 6. Activity Theory in the Context of Online Learning (Levy, 2006b)

Levy (2006b) defined an online learning activity as, "an educational procedure designed to stimulate learning by online experience utilizing online learning systems and tools" (p. 30). In the case of e-learning, the community is created through the e-learning system for the subjects. Likewise, the objects are the e-learning activities.

E-learning Activities

In e-learning systems, activities are completed by users as a means to assess the success of the user's outcomes (Lam, 2004). In Levy (2008), CVFs were used to identify

what e-learning activities offer the most value within an online learning system. Levy

(2008) defined CVFs as, "the factors that educational institutions should pay attention to

in order to increase the learners' perceived value, which in turn may help reduce dropout

in online learner courses" (p. 1664). Levy (2008) further categorized the findings by

grouping them into five CVFs: (a) Collaborative, Social, and Passive Learning Activities;

(b) Formal Communication Activities; (c) Formal Learning Activities; (d) Logistic

Activities; and (e) Printing Activities. Levy (2008) concluded that e-learning activities

within the first three categories (a, b, & c) have the highest perceived value within e-

learning systems, therefore, categories (d) and (e) are not included in this study. Table 3

depicts categories (a), (b), and (c) along with the e-learning activities used within the

Levy (2008) study.

Table 3. Adapted from List of the CVF on Online Learning Activities (Levy, 2008)

Category	Item Description
Collaborative, Social, and Passive Learning Activities	1. Participating in chat sessions (unofficial with other students) 2. Sharing my assignments with the other students (via discussion forum) 3. Sharing my assignments with other students (via e-mail) 4. Participating in chat session (official sessions with the professor) 5. Participating in live voice-chat sessions 6. Reviewing chapters slides online 7. Sending e-mails to other students 8. Reading other students' assignments (via discussion forum) 9. Listening to course audios online 10. Reading e-mails from other students

Table 3. Adapted from List of the CVF on Online Learning Activities (Levy, 2008) (continued)

Category	Item Description
Formal Communication Activities	1. Reading e-mails from the professor
	2. Reviewing professor's feedback on assignments (online)
	3. Sending e-mails to the professor
	4. Reading the professor's discussion forum messages
	5. Reading information off the school's site
	6. Checking grades online
	7. Register for courses online
	8. Reading assignments' guidelines online
	9. Checking for course(s) updates
Formal Learning Activities	1. Replying to students' discussion forum messages
	2. Posting new discussion forum messages
	3. Reading other student's discussion forum messages
	4. Submitting course(s)' assignments online
	5. Reviewing other students' personal Websites
	6. Developing personal Website, profile, or blog
	7. Replying to professor's discussion forum messages

Categories (a) and (b) have been traditionally classified as formative assessments.

Sadler (1989) described the purpose of formative assessments as a way to identify the gap

between current understanding and the desired goal by providing feedback, dialogue, and

non-assessed activities that can be developed into learning. Category (c) has been

traditionally classified as summative assessments. Rovai (2000) described summative

assessments as high-stakes assessments used for promotion, placement, certification, and

accountability in learning environments. As depicted in Table 4, e-learning in an

organizational context has grouped learning activities into similar categories' such as

instructional, collaborative, application, and assessment (Fry, 2001).

Table 4. Learning Management System Activities (Fry, 2001)

Categories	Learning Activities
Instructional	Deliver concepts
	Demonstrations
	Workshop content
	Reference articles
	Web links
Collaborative	Expert led chats
	Mentoring
	Peer-to-peer chat
	Discussions
	Mentored exercises
	Group meetings
Practice	Exercises
	Projects
	Lab work
	Simulations
Assessment	Performance testing
	Proficiency testing
	Certification testing
	Customized assessments

In additional to Levy's (2008) list of valuable learning activities, studies have identified

exams, quizzes, and course projects as critical summative assessments (Bailie & Jortberg,

2009). Bailie and Jortberg (2009) compiled a list of 10 broad categories of e-learning

assessments from 3,200 responses sorted by frequency of use depicted in Table 5.

Table 5. Types of Assessment on Online Learning (Bailie & Jortberg, 2009)

Responses	Frequency	Percent
Homework assignments	655	20%
Online tests and/or quizzes	606	19%
Bulletin-board postings	547	17%
Projects/papers	494	15%
Participation in chat room	313	10%
Proctored tests and/or quizzes	234	7%
Team projects	149	5%
Reflective journal	92	3%
Student portfolio	79	2%
Other	31	1%

E-assessments have been defined by the Joint Information Systems Committee (JISC) (2006) as, "the end-to-end electronic assessment processes where ICT [Information & Communications Technology] is used for the presentation of assessment activity and the recording of responses" (p. 43). Bailie and Jortberg (2009) stated that "proving identity in every situation that a student performs is not realistic, practical or cost effective" (p. 199). For the purpose of this study, items from Tables 3, 4, and 5 adapted from prior studies that meet the JISC (2006) definition of e-assessments that are either formative or summative, known collectively as e-learning activities, was included in the initial list for potential for impersonation fraud. Table 6 lists a summary of research studies and relevant literature on activity theory and e-learning activities.

Table 6. Summary of Research Studies on Activity Theory and E-learning Activity

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Bailie & Jortberg, 2009	Empirical	3200 assessments	Survey ranking top e-learning activities	E-learning activities fall into 10 broad assessment categories.

Table 6. Summary of Research Studies on Activity Theory and E-learning Activity
(continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Crawford, 2001	Theoretical	Commentary	Categorization of various activities within e-learning systems	Distributed learning environments are focusing away from the design of activities toward theoretical foundation to produce more successful outcomes.
Engeström, 2001	Exploratory	60 representatives of physicians, nurses, and staff	Case study to explore unit of analysis, multi-voicedness of activity, historicity of activity, contradictions as driving force of change in activity, & expansive cycles as principals of activity theory	There are contradictions in the outcomes of activities among the objects and goals. Suggested a complementary dimension to bring cohesion to subjects, tools and objects.
Frederickson, Reed, & Clifford, 2005	Experiment	16 first-term graduate students	Quantitative data measuring knowledge, anxiety, self-confidence, & learning experience as it relates to e-learning activities	Although the learners found Web-based activities effective, using activity theory allows learning outcomes to be evaluated from a systematic perspective.

Table 6. Summary of Research Studies on Activity Theory and E-learning Activity (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Hasan & Crawford, 2003	Exploratory	2 Universities	Case study understanding various activities when designing Web-based systems.	There are no simple information technology solutions for various activities. A framework would be useful to design tools to for specific activities.
Levy, 2006b	Exploratory	47 MIS students who attended five online focus group discussion sessions	Case study ranking tope e-learning activities	Identified top 10 most valuable e-learning activities based upon activity theory.
Levy, 2008	Empirical	214 graduate students	Survey to identify CVF for e-learning activities	Identified and ranked five critical value factors for 36 e-leaning activities.
Liu & Schwen, 2006	Exploratory	MBA course including 13 students	Case study to explore the constructs of activity theory (tools, rules, division of labor, & community) as it relates to e-learning activities	All components of activity theory such as tools, rules, division of labor, and community are necessary for successful implementation of policies for e-learning systems.

Table 6. Summary of Research Studies on Activity Theory and E-learning Activity (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Walker, 2004	Exploratory	A group of students in an online discussion	Case study exploring how tools affect the community within an e-learning activities.	Activity theory allows a closer look at goals for communication within e-learning systems and the specific types of technological tools necessary to stabilized them.

Impersonation Fraud

   E-learning institutions consider impersonation as a major concern because current

countermeasures can prove to be insufficient (Rowe, 2004). Impersonation is considered

the intentional collaboration between users with the intent to commit fraudulent behavior

by the misrepresentation of identity (Apampa et al., 2010). Weippl (2005) stated that

users of e-learning systems deliberately reveal their authentication details to others to

allow impersonation. Levy and Ramim (2010) identified impersonation fraud as one of

five common security attacks within e-learning systems.

   Passow, Mayhew, Finelli, Harding, and Carpenter (2006) examined the effects of a

number of independent variables on IS misuse based upon the type of learning activity

being assessed. Passow et al. (2006) found significant differences in potential IS misuse

depending on the value of learning activity being assessed. Brent and Atkisson (2011) as

well as Schmelkin, Gilbert, Spencer, Pincus, and Silva (2008) noted in their studies

significant differences in potential for IS misuse depended on the perceived severity of

seriousness for each e-learning activity and concluded that e-learning activities should not be lumped into a single category.

Lanier (2006) studied user's potential for IS misuse based on demographics of age, gender, and e-learning experience. Lanier (2006) observed consistent evidence that demographic differences appear to have a significant role in IS misuse. For example, males are more likely to commit IS misuse than females. Thus, the inability to confirm who is completing the e-learning activity via authentication is still a major concern in e-learning systems (Bailie & Jortberg, 2009; Hernandez, Ortiz, Andaverde, & Burlak, 2008). Apampa et al. (2010) suggested the issue of impersonation is related to the strength of the authentication method.

Because e-learning depends on the use of the Internet, e-learning is susceptible to a wider range of security risks (Alwi & Fan, 2010). Both the success and quality of the e-learning system relies on the certainty that the user who completes e-learning activities is authenticated (King et al., 2009). The problem, which has been expressed by numerous e-learning providers, is the risk of impersonation during the completion of e-learning activities that are used to assess user's knowledge (Alwi & Fan, 2010; Apampa et al., 2011). E-learning systems must ensure that users completing learning activities are legitimate (Oakley & Singh, 2011). This problem is prevalent in any organization where e-learning systems are used to provide training as a means to complete learning activities for summative assessments such as certifications exams (Kowalski, Wisniewski, & Beheshti, 2009). Masters and Ellaway (2008) developed an e-learning medical guide geared towards medical institutions that have made e-learning mainstream. They cautioned that impersonation fraud is a real ethical issue for medical students who use

e-learning systems. This review of impersonation fraud demonstrates that the value of

e-learning in the workplace is often studied from the perspective of meeting

organizational strategies in terms of user acceptance and performance outcomes,

however, these studies often fail to examine how critical it is to ensure the user

completing the activity is authenticated against threats of impersonation (Wang, Ran,

Liao, & Yang, 2010). Table 7 lists a summary of research studies and relevant literature

on IS misuse and impersonation fraud.

Table 7. Summary of Research Studies on Impersonation Fraud

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Apampa et al., 2010	Theoretical	Commentary	Discussion on classifying 3 types of impersona- tion fraud	Depending on the type of impersonation fraud, the solution for authentication must vary.
Apampa et al., 2011	Experimental	5 video sequences	Quantitative data measuring presence verification to deter impersona- tion fraud	Summative e- assessments are susceptible to impersonation fraud due to incomplete research on authentication and user identification.
Brent & Atkisson, 2011	Empirical	401 students	Survey measuring motivation & deterrence of IS misuse	E-learners choose whether or not to conduct IS misuse depending on the perceived importance of the activity being completed. Not all activities have the same risk of IS misuse.

Table 7. Summary of Research Studies on Impersonation Fraud (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Hernandez et al., 2008	Experiment	102 high school students	The use of biometric authentication to reduce deliberate impersona-tion fraud	Even with the use of biometrics, 20% of users still found a way to intentionally fake authenticating their identity.
King et al., 2009	Empirical	121 undergradu-ate students	Survey measuring perceived attitudes toward impersona-tion fraud within e-learning systems	73.6% perceived it is easier to cheat online than in traditional learning settings.
Lanier, 2006	Empirical	1262 undergradu-ate and graduate students	Survey measuring self- & peer-reported IS misuse within traditional face-to-face learning environments versus e-learning environments	The rate of online IS misuse exceeds the traditional learning environment. Continued exploratory research is necessary to reduce the percent of IS misuse in e-learning systems.
Levy & Ramim, 2010	Empirical	519 undergradu-ate and graduate online students	Survey measuring perceived ethical severity of the five e-learning security attacks	Deliberately impersonating other student's accounts for one of the severe security attacks.

Table 7. Summary of Research Studies on Impersonation Fraud (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Masters & Ellaway, 2008	Theoretical	Commentary	Defining impersonation fraud & implications within e-learning systems	Guide discussing that impersonation fraud is a real concern in e-learning systems and suggested solutions to reduce the risk by implement appropriate authentication.
Oakley & Singh, 2011	Exploratory	Interviews e-learning students (sample size not given)	Case study exploring ethical-decision making in the e-learning environment specific to impersonation fraud	Identified impersonation fraud as a significant factor.
Passow et al., 2006	Empirical	695 undergraduate and graduate students	Survey measuring IS misuse for both formative & summative assessments	Found a significant difference toward IS misuse based upon the value of the activity. 36% conduct IS misuse on summative assessments and 14% for formative assessments.
Rowe, 2004	Theoretical	Commentary	Discussion on the threat of impersonation fraud in e-learning	E-learning assessments have serious security risks. Countermeasures insufficiently reduce the risk of impersonation.

Table 7. Summary of Research Studies on Impersonation Fraud (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Schmelkin et al., 2008	Empirical	560 undergradu-ate students	Survey measuring IS misuse on assessment type & perceived seriousness of behavior	Student differentiate the severity of IS misuse based on type of assessment being completed. Situational factors need to be considered when planning to reduce risk of IS misuse.
Weippl, 2005	Theoretical	Literature review	Describes the nature of e-learning & security threats that are critical to address	E-learners deliberately reveal their authentication details to allow impersonation.

Authentication

ISs must be secured against misuse (D'Arcy et al., 2009). Preventative measures are

active system controls used to prevent IS misuse from users both inside and outside the

system (Straub & Nance, 1990). Authentication controls are considered preventative

layer tools to protect against IS misuse (D'Arcy et al., 2009; Straub & Nance, 1990).

Authentication is a critical preventative control used in Web-based systems in order to

determine the identity of users (Helkala & Snekkenes, 2009). Authentication controls

have various factors used to authenticate users such as something the user knows (e.g.

passwords), something the user has (e.g. tokens), or something the user is (e.g.

biometric), which served as a framework for this exploratory study (Furnell, 2007).

Selection of suitable authentication controls is important due to the issues of usability and cost (Helkala & Snekkenes, 2009). Often, the choice is left to third-party vendors who offer a 'one size fits all' solution only protects one aspect of the system (Yang & Padmanabhan, 2010). Helkala and Snekkenes (2009) argued that the complexity in selecting suitable authentication controls is due to the number of alternatives available. Due to this complexity, Helkala and Snekkenes (2009) developed a framework, shown in Figure 7, to select the most suitable authentication method to comply with usage and environment-related requirements to meet specific scenarios.
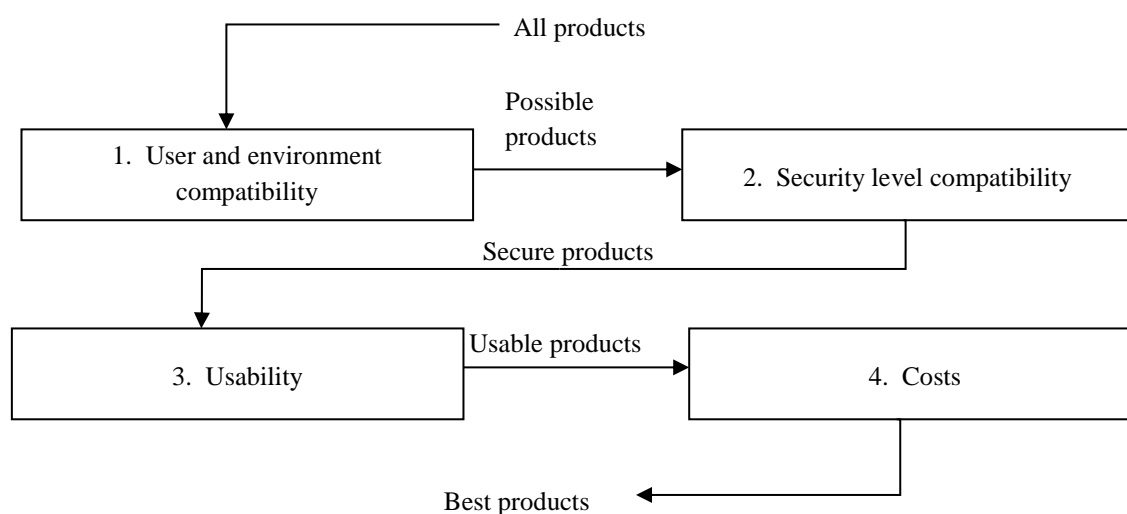
Figure 7. A Framework for Selecting the Most Suitable Authentication Method (Helkala & Snekkenes, 2009)

They argued that not all usage scenarios need the same levels of authentication strength and organizations need to assess the threat of IS misuse for various activities when selecting authentication methods in order to identify the suitable authentication strength (Helkala & Snekkenes, 2009).

Suitable authentication controls have been investigated for Web-based systems in e-banking, e-government, and non-academic e-learning systems. Hutchinson and Warren (2003) introduced an e-banking framework using a list of security requirements to authenticate users based upon the level of risk for the activity being performed. Howell and Wei (2010) completed a study to identify common e-banking activities and the current level of authentication strengths typically used to reduce IS misuse. They concluded that more research needs to be done to "analyze each e-business item in detail" (Howell & Wei, 2010, p. 78) so the sufficient authentication controls can be implemented. This shows that research for Web-based systems has recognized the importance of identifying suitable levels of authentication strength for specific activities based upon a perceived threat from IS misuse.

The standards council for financial institutions urged financial institutions apply an "appropriate and reasonable" authentication strength specific for the type of activity (Council, 2011, p. 4). Kim and Hong (2011) improved the user authentication strength system used for federal systems by listing the diversity of authentication methods and suggested a process to select authentication strength based upon the activity type within Web-based systems. These studies showed that not all activities need the same authentication strength. Suitable authentication strength for different activities within Web-based systems is a major concern for organizations in order to secure the system from IS misuse such as impersonation fraud.

Authentication Strength

Authentication strength is measured by the combinations of the number and the type of authentication factors used to identify a remote system user (Asha & Chellappan,

2008; O'Gorman, 2003). Single-factor authentication is a username/password or personal identification number (PIN), a token, or a single biometric. Each factor can be considered weak or strong depending upon the situation. For example, passwords, PINs, and tokens are a weak authentication against brute force guessing because it is likely to be guessed. Additionally, they are a weak authentication for deliberate impersonation fraud because they can easily be given out (O'Gorman, 2003). Any biometric factor by itself is considered a stronger authentication control than a password, PIN, or token because of its uniqueness, however, it can become weak if an individual deliberately provides biometric credentials to someone else so they can perform activities under their identity (O'Gorman, 2003)

Combining single-factors into a multi-factor authentication is often done to strengthen security (O'Gorman, 2003). A multi-factor authentication combines two or more factors. For example, a token that generates a onetime password using both something a user knows can be combined with something that a user has such as a smartcard, USB device, or a unique system generated password to create a two-factor authentication (O'Gorman, 2003). Three-factor authentication combines each of the factors; a secret, a token, and a biometric to authenticate the user, while it is considered to be the strongest authentication control (Al-Khouri & Bal, 2007).

Authentication strength cannot be expressed in absolute measures, thus, the strength of a factor is measured relatively to other factors based on the ability to reduce the threat (O'Gorman, 2003). Hence, when discussing authentication strength, factors should be considered stronger or weaker than other factors based upon the context they are described (O'Gorman, 2003). For example in e-banking, the Federal Financial Institution

Examination Council, the standards council for financial institutions, considered single-factor authentication inadequate for high-risk activities and recommends multi-factor authentication as a reasonable mitigation to risks (Council, 2001). Caloyannides, Copeland, Datesman, and Weitzel (2003), equally stated that not all activities in e-government systems require the same level of authentication. As stated by Caloyannides et al., (2003), "higher-risk activities require higher levels of authentication" (p. 17). The National Institute of Standards and Technology (NIST) developed publication 800-63-2 that identified four levels of authentication; (1) identity proofing and registration including the delivery of credentials, (2) tokens for proving identity, (3) remote authentication mechanisms, and (4) assertion mechanisms (Burr, Dodson, Newton, Perlner, Polk, Gupta, & Nabbus, 2013). Level 1 consists of the use of single-factor authentication such as passwords and PINs. Level 2 consists of single-factor authentication through the use of a token or biometric. Level 3 authentication combines Level 1 and 2 into a multi-factor authentication. Level 4 authentication is the highest level and relies on encrypted multi-factor authentication methods from factors used in Levels 1 − 3 (Burr et al., 2013). These studies demonstrated that organizations have recognized the need for different authentication levels for diverse activities not only in e-learning systems, but within Web-based systems in general.

Single-factor Authentication

Due to the ease of use and high user acceptance, single-factor authentication such as username/password, a token, or a biometric is most commonly used to authenticate users within IS (Graf, 2002). Passwords are secrets that are known only to a user and are often combined with a username in order to gain access to a system. Because passwords can be

easily distributed, this authentication method is often considered inadequate to protect critical e-learning activities from impersonation fraud (Apampa, Wills, Argles, & Marais, 2008). For example, a study by Kruck and Teer (2008) investigated IS misuse using 350 students and found that 62% of students deliberately intended to engage in IS misuse by distributing their passwords.

Tokens are stored information about one or more authentication methods such as username/password or biometric identifiers (Bolle et al., 2003). Because tokens create passwords made up of longer streams of numbers to secure the system, it is considered a stronger authentication than passwords that must be shorter in order to be memorized (Bolle et al., 2003). Tokens can be physical such as keys, smartcards, or digital certificates.

Digital certificates are issued by a certification authority and have been implemented in e-learning where, "certificates represent a trusted party" (El-Khatib, Korba, Xu, & Yee, 2003, p. 11). Due to the ease of transferability, Graf (2002) found that the use of tokens alone for user authentication is not always viable in e-learning activities to protest against impersonation fraud. Thus, if a user wishes to have someone else do an activity for them; the token can be given to that individual. Tokens are more reliable when combined with other authentication factors (O'Gorman, 2003).

Biometrics is defined as the identification of an individual based on physiological and behavioral characteristics (Gao, 2012). Biometrics is based upon the uniqueness of a user's characteristics. Rabuzin, Bača, and Sajko (2006) advocated that biometric authentication is a stronger authentication than simply using passwords to access Web-based systems. In theory, this is due to the fact that a biometric is something that a user

has, which cannot be taken and, therefore, provides non-repudiated proof of identity (Rabuzin et al., 2006).

There are many biometric characteristics that have been proposed for use in e-learning systems. Gao (2012) as well as Asha and Chellappan (2008) listed common physiological biometrics used for authentication: fingerprint, palm print, facial recognition, iris; and common behavioral biometrics used for authentication: keystroke, voice, and signature. Although the use of biometric authentication has increased in popularity over traditional methods such as the use of passwords alone, Levy and Ramim (2009) stated that "there is a recent trend in biometric practice to integrate more than a single biometric method of authentication in order to increase its accuracy, transparency, and reliability" (p. 383). Moini and Madni (2009) cautioned on privacy implications and stated that "facial images, voiceprints and 'latent' fingerprints left on surfaces of objects can be taken without a person's knowledge or consent" (p. 471).

Hernandez et al. (2008) challenged that there is still an inability to authenticate the user throughout the duration of an activity by using a single-sign on biometric authentication. Apampa at el. (2011) as well as Levy and Ramim (2007) warned that biometric authentication may only deter impersonation and that an imposter can take over the activity once the biometric is matched. Levy and Ramim (2007) went on further by proposing a theoretical approach for the use of biometric fingerprint tools to randomly and continuously validate user. Although, Levy and Ramim (2007) research focused solely on e-exams, Levy and Ramim (2009) concluded that "there are other e-learning activities beyond e-learning exams that provide significant credit for students towards their final course grade, such as discussion forums and assignment submissions" (p. 382).

They noted that such e-learning activities are susceptible to impersonation and could benefit from the use of continuous biometric authentication or other strong authentication.

Multi-factor Authentication

   To improve authentication strength, two single-factor authentications can be combined into a two-factor authentication (Gao, 2012). It is more difficult to compromise a two-factor authentication than a single-factor authentication (Howell & Wei, 2010). Bhargav-Spantzel, Squicciarini, and Bertino (2007) explored the use of two-factor authentication in an identity management system and argued, "the second authentication combines several authentication factors in conjunction with the biometric to provide a strong authentication" (p. 63). Two-factor authentication is most widely used in an Automatic Teller Machine (ATM), which requires the user to use both a PIN and an ATM card in order to complete the transaction (Council, 2001). In respects to e-banking, Schneier (2005) challenged that two-factor authentication is sufficient for use of local networks but is not sufficient to protect Web-based systems from impersonation fraud.

   In their study Al-Assam, Sellahewa, and Jassim (2011) found that using a secret key, such as, a password and a biometric authentication such as a fingerprint or face recognition improves security over a single-factor authentication. Similarly, Rathgeb and Uhl (2010) used the addition of biometric authentication iris recognition along with a username/password in a case study to support the use of two-factor authentication to reduce threats of impersonation fraud. Rathgeb and Uhl (2010) purported that although iris recognition is a successful way of continuously identifying the user during an activity, there are performance issues of recognition rates when this biometric

authentication is used in Web-based systems. Two-factor authentication still contains the inherent risk of impersonation because the user can distribute both the username/password and sign-on with a biometric match allowing the legitimate user to be impersonated (Bhargav-Spantzel et al., 2007).

Another more recent two-factor authentication approach is the use of live-proctor authentication along with username/password or biometric authentication. Live-proctor authentication is the observation of remote e-learners via a Web-cam and a live proctor over the internet, irrespective of the location (Kitahara et al., 2011). Bedford et al. (2009) completed a case study using Remote Proctor[tm] from Software Secure to use fingerprint biometrics to authenticate 31 students during an e-exam along with 20 faculty participants who monitored the activity and concluded that both, students and faculty, agreed that biometric and live-proctor authentication could reduce IS misuse. In their case study, Rodchua et al. (2011) compared the reliability and accuracy of live-proctor authentication tools such as Remote Proctor[tm], which uses biometric and live-proctor authentication as well as ProctorU and ProctorCam, which uses username/password and live-proctor authentication. Rodchua et al., 2011 purported that the use of biometric and live-proctor authentication has more strength than username/password and live-proctor authentication.

O'Gorman (2003) posited that "generally, multi-factor authentication that combines all three factors has not been widely applied, although some high security applications may require this" (p. 7). Studies have reported that multi-factor authentication combining three authentication factors, creates a stronger authentication improving reliability against impersonation fraud (Bolle et al., 2003). Howell and Wei (2010) expressed the

importance of using three-factor authentication in organizations such as e-finance by stating that "banks that have not yet addressed the need for multi-factor authentication should have that at the top of their [information technology] priority lists" (p. 73). Al-Khouri and Bal (2007) argued that three-factor authentication is essential for e-government and e-commerce activities because it "addresses the need for strong user authentication of virtual identities" (p. 361). Similarly, Rodchua et al., 2011 argued, "creating multifaceted layers of devices can be an appropriate approach for the implementation" (p. 7). Table 8 lists a summary of research studies and relevant literature on authentication.

Table 8. Summary of Research Studies on Authentication

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Al-Assam et al., 2011	Empirical	3 data sets	Case study evaluating the trade-off between high accuracy & security of multi-factor authentication	The security of a single-factor biometric can be undermined. Securing against impersonation using stronger multi-factor authentication has benefits.
Al-Khouri & Bal, 2007	Experiment	2 data sets	Quantitative analysis on the tradeoff between accuracy & security in two-factor authentication	Stronger authentication such as multi-factor must become the foundation for Web-based systems to secure identity and reduce impersonation fraud.
Apampa, Wills, Argles, & Marais, 2008	Exploratory	3 Scenarios	Discussion on improving integrity by securing e-assessments	Username and passwords alone do not reduce the risk of impersonation.

Table 8. Summary of Research Studies on Authentication (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Asha & Chellappan, 2008	Meta-analysis	IEEE security models	Compared standard features of each model in order to propose a new model to authenticate users in e-learning systems	The use of multi-factor authentication in lieu of a single biometric factor offer stronger authentication for identity to reduce impersonation.
Bedford et al., 2009	Experiment	20 faculty & 31 students	Study to measure acceptance & adoptions of live-proctor authentica- tion	48% of students that the use of live-proctor authentication can reduce IS Misuse. Faculty addressed technology issues as a challenge for its implementation.
Bhargav-Spantzel et al., 2007	Exploratory	2 biometric protocols	Study comparing 2 protocols to compare multi-factor authentica- tion strength	Each additional factor adds strength to the authentication.
Caloyannides et al., 2003	Theoretical	Commentary	Outlines authentication strength for individual activities	E-government systems must ensure that no one impersonates another and the challenge is to recognize which transactions require stronger authentication.

Table 8. Summary of Research Studies on Authentication (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Council, 2011	Theoretical	Authentica-tion guide-lines	Outlines authentication strength for individual activities	The level of authentication strength should be suitable to the risk associated to the service or product it is securing.
Gao, 2012	Empirical	13 online students	Case study to measure the effectiveness of live-proctor authentication to deter IS misuse	2 students out of 13 were identified from live-proctor authentication as possible IS misuse behavior in an e-learning system.
Graf, 2002	Exploratory	None	Discussion on the use of CIPRESS monitoring software to authenticate using live-proctor authentication during summative assessments in an e-learning system	Single-factor authentication such as username and password do not securing against impersonation in e-learning. Live-proctor authentication is one solution to ensure identity.

Table 8. Summary of Research Studies on Authentication (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Helkala & Snekkenes, 2009	Exploratory	11,000 hospital employees	Case study ranking authentication methods based user & environment, security level compatibility, usability, & cost	Organizations often select a single authentication method, which leads to poor decisions. A tool to rank authentication methods according to scenario usage is more beneficial.
Hernandez et al., 2008	Experiment	102 high school students	Case study to measure effectiveness of biometric authentication to deter IS misuse	78% of students agree biometric authentication such as face recognition should be implemented during e-learning assessments to deter IS misuse.
Howell & Wei, 2010	Exploratory	20 banks Websites	Ranked e-banking activities & adoption rates of authentication	Securing Web-based e-banking activities with specific authentication strength has not been addressed by institutions effectively.
Hutchinson & Warren, 2003	Exploratory	E-banking scenarios	Case study to identify a correlation between adequate authentication mechanisms & e-banking scenarios	There is a need to develop an authentication framework for specific e-banking transactions to provide adequate authentication.

Table 8. Summary of Research Studies on Authentication (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Kim & Hong, 2011	Exploratory	User authentication level system	Discussion on how to select suitable authentication using user authentication models to reduce risk of impersona- tion	Included multi-factor authentication to traditional authentication levels to increase identity security for activities requiring high confidence level for online user identity.
Kitahara et al., 2011	Exploratory	Students in an e-learning course (sample size not stated)	Case study to measure the reliability & accuracy of the use of live-proctor authentication along with username/ password or biometric authentication	The use of two-factor authentication using live-proctor and biometric authentication is stronger than using live-proctor and username/password authentication.
Kruck & Teer, 2008	Empirical	350 undergradu- ate students	Survey measuring perceptions of IS misuse using single- factor authentication	62% of students deliberately intended to engage in IS misuse by distributing their passwords.
Levy & Ramim, 2007	Theoretical	Commentary	Discussion on effectiveness of biometric authentication against impersona- tion	Proposes a biometric authentication solution to reduce impersonation during e-learning exams, but may only deter an imposter.

Table 8. Summary of Research Studies on Authentication (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Levy & Ramim, 2009	Empirical	98 non-IT students	Survey measuring perceived ease-of-use, perceived usefulness, intention to use, code of conduct awareness & ethical decision making	A single biometric authentication is not suitable for all the needs of an e-learning system. Multi-biometrics would be a better fit is certain situations.
Moini & Madni, 2009	Theoretical	Exploratory	Discussion on the use of continuous authentication to reduce risk of impersona- tion.	Single-factor, one- time authentication does not reduce risk of impersonation. Continuous authentication can be an effective prevent and protect against impersonation attacks.
O'Gorman, 2003	Empirical	Security attacks and authentication mechanisms	Compares authentication against potential attacks to measure suitability	Appropriate authentication strength is dependent upon situational factors.
Rabuzin et al., 2006	Empirical	300 e-learners	Survey measuring usability & user satisfaction of biometric authentication	Although 76% found the technology ease to use, multi-factor biometrics is underutilized in e-learning systems for certain activities.

Table 8. Summary of Research Studies on Authentication (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Rathgeb & Uhl, 2010	Experiment	100 templates	Case study evaluating accuracy of multi-factor biometric authentication	Although iris recognition has a 5.61% false rejection rate, it is a successful way of continuously identifying the user during an activity.
Schneier, 2005	Theoretical	Commentary	Discussion on multi-factor authentication strength	Challenged that two-factor authentication is sufficient for use of local networks but is not sufficient to protect Web-based systems from impersonation fraud.
Yang & Padmanabhan, 2010	Empirical	50,000 user-centric sessions	Case study measuring user identification accuracy using various multi-factor authentication	10.13% increase in accuracy with the addition of more authentication factors.

Task-Technology Fit

To gain a further understanding of how to evaluate e-learning activities within Web-based systems and the selection of a suitable level of authentication to protect against impersonation, it is useful to research a theory focused on perceived fit. Theories on fit in the literature were originally centered on organizational theory that measured individual ability and job satisfaction (Goodhue & Thompson, 1995). Lin (2012) identified three dimensions on how perceived fit should be measured in an IS context; usefulness (does the system function the way it's needed), usability (can users work with the system

successfully), and likeability (do users feel the system is suitable). Goodhue (1988)
studied general fit theory focusing on tasks, system characteristics, as well as
performance and proposed that there was a positive impact on performance only when
there is a correspondence between functionality and tasks.

Goodhue and Thompson (1995) elaborated on the formal construct known as TTF to
explain the need for the fit in IS between both the tasks and technologies used to achieve
a successful outcome. Goodhue and Thompson (1995) defined a task as, "actions carried
out by individuals in turning inputs into outputs" and technology as, "tools used by
individuals in carrying out their task" (p. 216). TTF proposes that the better the fit
between task and technology, the more position the outcome within the system (Staples
& Seddon, 2004). Dishaw and Strong (1999) discussed the theoretical foundations of the
TTF construct as, "the matching of the capabilities of the technology to the demands of
the task" (p. 11). The TTF model is shown in Figure 8.
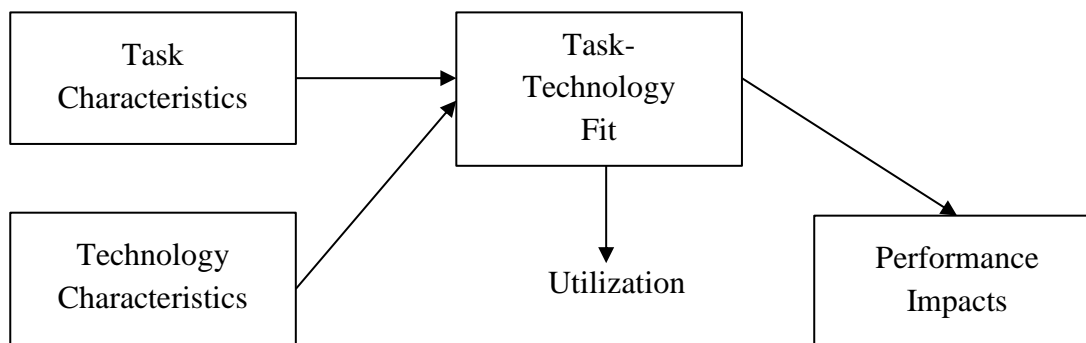
Figure 8. Task-Technology Fit Model (Goodhue and Thompson, 1995)

The TTF model used in the study of IS often measures the additional construct of
utilization (Dishaw & Strong, 1999). Utilization is measured by predicting attitudes of
users and beliefs about the use of technology (McGill & Klobas, 2009). For example,
McGill and Klobas (2009) conducted a study and found that TTF is a factor that has a

positive influences on the desired outcomes expected within an e-learning system,

however, their study assumed system utilization was voluntary. The TTF model where

utilization is measured suggested that in order for a task to be used, the technology must

fit the task (McGill & Klobas, 2009). However, McGill and Klobas (2009) study of

utilization assumed the use of technology is voluntary. Because the use of authentication

is not voluntary for users when accessing secured systems, measuring perceived

utilization as part of the TTF model is outside the scope of this study. Goodhue and

Thompson (1995) argued that user evaluation is a sufficient surrogate of TTF also in

mandatory systems. Gebauer and Ginsburg (2009) further posited that "user-perceived

'overall technology evaluation' is viewed as a general indicator of fit" (p. 130). Thus, for

the purpose of this study, the model develop by Goodhue and Thompson (1995) was used

to understand the fit between e-learning activities and the suitable level of authentication

perceived by users, as well as perceived by users that their peers will identify to reduce

impersonation. Table 9 summarizes the relevant studies on the use of the TTF model as a

framework for selecting technology to fit specific tasks.

Table 9. Summary of Research Studies on Task-Technology Fit

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Dishaw & Strong, 1999	Empirical	60 maintenance projects	Study comparing technology utilization using technology acceptance model, TTF & a combination of both suing path analytics	Expanding the technology acceptance model with TTF constructs assist in selecting appropriate technology for individual tasks

Table 9. Summary of Research Studies on Task-Technology Fit (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Gebauer & Ginsburg, 2009	Empirical	144 user reviews	Study measuring technology performance, task-related fit, & content-related fit	User's overall technology evaluations were significant regarding the overall fit between technology and factors related to user tasks and use context.
Goodhue & Thompson, 1995	Empirical	662 non-IS employees	Study measuring technology utilization and fit with tasks it supports	In order for the IT to be successful, it must be a good fit with the task it supports and the TTF model is a good diagnostic tool for organizations to evaluate if the technology is meeting their needs.
Lin, 2012	Empirical	165 undergradu-ate students	Survey measuring perceived fit & satisfaction for e-learning activities	Perceived fit and satisfaction are significant when implementing technology in an e- learning environments. Educational institutions need to continue using the TTF to improve IS success.
McGill & Klobas, 2009	Survey	267 undergradu-ate students	Utilization, attitudes toward use, social norms, & performance impacts in e-learning systems	TTF has a strong positive influence on performance impact and plays an important role in the success of E-learning systems.

Table 9. Summary of Research Studies on Task-Technology Fit (continued)

Study	Methodology	Sample	Instruments/ Constructs	Main Findings
Staples & Seddon, 2004	Empirical	140 librarian (mandatory users), 308 students (voluntary users)	Survey measuring TTF, utilization, performance impacts, social norms and attitudes toward use for both voluntary & mandatory use of systems	The fit of the technology is more significant than utilization; therefore, with mandatory use of technology utilization is irrelevant.

Summary of What is Known and Unknown in Research Literature

A review of the literature has described the complexities organization face in selecting

authentication controls to secure their e-learning system activities from impersonation

fraud. This literature review has shown a consensus that a substantial amount of research

has been done regarding authenticating methods in e-learning systems. What is known

included levels of authentication controls available as well as the strengths and

weaknesses of each of the authentication controls for Web-based systems. Furnell (2007)

provided a definition of authentication that serves as a framework for authentication

factors, which are classified into weak versus strong authentication. Literature has shown

that Web-based systems are susceptible to IS misuse even when acceptable authentication

controls are implemented (Kerka & Wonacott, 2000). IS misuse includes the risk of being

unable to confidently identify the user participating in e-learning activities after the initial

authentication into the system. This type of IS misuse has been defined in the literature as

impersonation fraud and is a prevalent issue faced by all organizations who offer e-learning.

There has been much research conducted about user authentication in Web-based systems, however, the area of suitable authentication for e-learning activities is not fully explored (Marais et al., 2006). Weippl (2005) purported that not all e-learning activities are equal in terms of authenticating and validating the user completing the e-learning activity is warranted. Summative versus formative activities have different implications if susceptible to impersonation. Apampa et al. (2010) expressed the need for additional research on how to authenticate critical e-learning activities specifically from impersonation, but did not identify what strength of authentication needs to be used for each given activity. This study took an exploratory approach to identifying specifically what e-learning activities were susceptible to impersonation and what levels of authentication controls were suitable to identify users in diverse e-learning activities. It was evident from prior research, that the evaluation of user perception of fit between a suitable technology and tasks for a desired outcome was relevant for this study. Specifically in this study, the technology was the authentication strength and the tasks were the e-learning activities. The fit between authentication strength and e-learning activities were an acceptable surrogate for fit when a desired outcome was expected such as reducing impersonation fraud (Gebauer & Ginsburg, 2009; Goodhue & Thompson, 1995).

Chapter 3

Methodology

Research Design

The research goal of this study was to empirically investigate what levels of

authentication methods and strength users perceived to be most suitable for activities in

e-learning systems based on the threats of impersonation. This study proposed to conduct

an exploratory research design to develop an instrument to measure users' perceptions

about suitable authentication methods. Following the initial development of a survey

instrument based upon the literature (phase 1), expert panel feedback was gathered for

instrument validity using the Delphi methodology. The initial instrument was adjusted by

adding or removing e-learning activities or adjustments to the scale for level of

authentication strength (phase 2). The finalized survey instrument was used to collect

quantitative data for analyses (phase 3). A link to a Web-based survey instrument was

e-mailed to a random sampling of individuals who were using an e-learning system to

collect relevant data about e-learning activities that they perceived and perceived by them

that their peers would identify to have high potential for impersonation. Additionally, the

survey instrument collected relevant data on what levels of authentication strength users

perceived and perceived by users that their peers would identify to be most suitable

against the threats of impersonation for the assessed e-learning activities. The goal of

asking users to assess the e-learning activities and strength of authentication as self-

reported as well as those that users perceived that their peers would identify, was to

measure if there were any statistically significant differences between each set of

responses for the surveyed e-learning activities.

Instrument Development

The Web-based survey that this study used collected anonymous data from each

respondent regarding their own perception and their perception that their peers would

identify the potential for impersonation. Also, data from each respondent regarding their

own perception and perceived by users that their peers would identify what levels of

authentication strength were suitable for assessed e-learning activities. Emailing is

considered a less costly, efficient, and appropriate solicitation method for Web-based

surveys to reach a large number of potential respondents in a given population (Fricker,

Galesic, Tourangeau, & Yan, 2005). The survey instrument contained measurement items

adopted from prior relevant studies from Levy (2006b) and Levy (2008) whose studies

developed instrument surveys to collect as well as analyze data resulting in a list CVFs of

e-learning activities. This survey instrument also contained measurement items adopted

from Bailie and Jortberg (2009) whose study evaluated the frequency of 10 broad

categories that e-learning providers used within non-academic systems. All categories

that were formative or summative in nature were retained for use in this study. Items not

used as an e-assessment were not included in the instrument as they are beyond the focus

of this study. Demographic variables such as gender, age, and e-learning experience were

also collected to measure if there were any significant differences between respondents

based upon those variables, while ensuring that the sample collected was a good

representation of the population. Qualtrics, a Web-based survey development tool, was

used to design the survey for the sample population.

Kankanhalli, Teo, Tan, and Wei (2003) indicated that using items adapted from prior

studies will enhance validity or, if necessary, new items can be developed based on

review of IS literature. E-learning activities *perceived by users to have a high potential*

for threats of impersonation (UP-HPI) and e-learning activities *users perceived that their*

peers will identify to have a high potential for threats of impersonation (PP-HPI) were

measured using 18 e-learning activities adapted from prior studies as identified in Table

10 (Bailie & Jortberg, 2009; Levy 2006b; Levy, 2008) (RQ1a & RQ1b).

Table 10. E-learning Activities Adapted from Bailie and Jortberg (2009), Levy (2006b),
and Levy (2008)

E-Learning Activities
1. Develop a personal Website, profile, or blog
2. Participate in text-chat sessions (official with professor)
3. Participate in text-chat sessions (unofficial with other students)
4. Participate in live voice-chat sessions (official with professor)
5. Participate in live voice-chat sessions (unofficial with other students)
6. Post a new discussion forum message (official to the professor)
7. Post a new discussion forum message (unofficial to other students)
8. Reply to discussion forum messages (official to the professor)
9. Reply to discussion forum messages (unofficial to other students)
10. Send e-mails to the professor
11. Send e-mails to other students
12. Share assignments with other students (via discussion forum)
13. Share assignments with the other students (via e-mail)
14. Submit assignments online
15. Submit exams online
16. Submit quizzes online
17. Submit ungraded practice quizzes online
18. Submit projects online

Authentication strength perceived by users to be most suitable against the threats of

impersonation (UP-ASI) for these assessed e-learning activities and *authentication*

strength perceived by users that their peers will identify to be most suitable against the

threats of impersonation (PP-ASI) for these assessed e-learning activities were measured using the same list of e-learning activities from UP-HPI and PP-HPI (RQ2a & RQ2b). Responses from UP-HPI and PP-HPI as well as UP-ASI and PP-ASI were measured to see if there were any significant differences perceived by users than those they perceived that their peers will identify (RQ1c & RQ2c). Significant components from responses from UP-HPI, PP-HPI, UP-ASI, and PP-ASI were identified using Exploratory Factor Analysis via Principal Component Analysis to answer RQ3a, RQ3b, and RQ3c. Additionally, demographic variables were measured to determine if there were any significant differences based on *gender* (DEM1) (RQ4a), *age* (DEM2) (RQ4b), and *e-learning experience* (DEM3) (RQ4c) using data gathered from responses for RQ1a, RQ1b, RQ2a, and RQ2b.

Validity and Reliability

Campbell (1957) evaluated the importance of both internal and external validity. Internal validity is whether the research made a significant difference in the specific study. Ellis and Levy (2009) indicated that internal validity is based on rather or not the design and the data allowed for accurate conclusions from the researcher. Straub (1989) indicated that instrument validity leads to improved internal validity. Instrument validation is maximized by content validity, construct validity, and reliability. Table 11 lists the requirements the questions Straub (1989) expressed that each should ask.

Table 11. Instrument Validation (Straub, 1989)

Validity Type	Question
Content Validity	Are instrument measures drawn from all possible measures of the properties under investigation?
Construct Validity	Do measures show stability across methodologies?
Reliability	Do measures show stability across the unit of observations?

Other threats to internal validity include maturation, history, and mortality (Hsu, Lee, & Straub, 2012). In order to mitigate internal validity, this study, used items for the survey that were validated in previous research studies (Bailie & Jortberg; Levy, 2006b; Levy, 2008). Because this study was exploratory and not experimental, mortality was not a threat since there was no control or treatment group being used (Sekaran, 2003).

The survey contained three sections (Section A, B, & C) and is available in Appendix A. To answer RQ1a and RQ1b, Section A asked respondents to rate the following for the e-learning activities listed in Table 10:

- I think this e-learning activity has a high potential for impersonation fraud by users, and
- I think my peers will identify that this e-learning activity to have a high potential for impersonation by users.

Section A used a 7-point likert scale ranging between the positive and negative extremes (1) 'Strongly Agree', (2) 'Agree', (3) 'Somewhat Agree', (4) 'Neither Agree or Disagree', (5) 'Somewhat Disagree', (6) 'Disagree', to (7) 'Strongly Disagree'.

Instrument validity is vital in order to substantiate theoretical findings and conclusions in information science (Straub, 1989). This scale was validated by Dolnicar and Grün (2013) who concluded that a 7-point likert scale showed the highest stability among responses compared to other formats as well as Cicchetti, Showalter, and Tyrer (1985) who concluded that there is a steady increase in instrument reliability up to 7-point likert

scale and the use of scales using three to six points will suffer. Cicchetti et al. (1985)

further noted that increases beyond 7-point likert scale render the difference in the results

as trivial.

To answer RQ2a and RQ2b, Section B asked respondents to rate the following for the

e-learning activities listed in Table 10:

- I think the selected Authentication Strength is suitable for the e-learning activity to reduce impersonation fraud, and
- I think my peers will identify the selected Authentication Strength as suitable for the e-learning activity to reduce impersonation fraud.

Section B used a 7-point likert scale ranging between weak and strong authentication

extremes (1) 'Extremely Low Strength', (2) 'Very Low Strength', (3) 'Low Strength, (4)

'Moderate Strength', (5) 'High Strength', (6) 'Very High Strength', to (7) 'Extremely

High Strength'. The purpose of using relative authentication strength terms such as 'low

or 'high' strength was "to identify combinations that complement strengths and reduce

weaknesses against different attacks" (O'Gorman, 2003, p. 4). Using the Delphi

methodology, an expert panel feedback was gathered to review the scale on

authentication strength used in the instrument (Okoli & Pawlowski, 2004). Adjustments

to the scale were made based upon the feedback for validity of the instrument scale.

In order to answer RQ4a, RQ4b, and RQ4c, the survey collected demographic data on

gender, age, and e-learning experience. Figure 9 illustrates Section C, which asked

respondents to choose from categorical, mutually exclusive choices for gender, age, and

e-learning experience.

Demographic Information

DEM1 What is your gender?

○ Male
○ Female

DEM2 What is your age?

○ Under 20
○ 20 - 29
○ 30 - 39
○ 40 - 49
○ 50 - 59
○ 60 or Over

DEM3 How many online classes have you completed?

○ None
○ 1-5
○ 6-10
○ 11+

Figure 9. Illustration of Demographic Measures for Survey

Construct validity is the extent that the variables are measuring the same thing from other validated empirical research analyses and in fact measure concepts that it claims to measure (Boudreau, Gefen, & Straub, 2001; MacKenzie, Podsakoff, & Podsakoff, 2011). Construct validity is obtained by allowing experts in the field familiar with the content to evaluate the instrument until a consensus on the content is agreed upon mutually (Straub, 1989). In order to ensure construct validity, an expert panel was organized to conduct a pre-screening of the instrument and recommended changes were applied until the instrument was approved by the panel for distribution. Another way to ensure construct validity is through factor analysis, which measures convergence validity by demonstrating high correlations on components measure the same construct and low correlations on components with significant differences (Straub, 1989). Factor analysis was done to see if there were any significant components of the potential for high

impersonation perceived by users and those perceived by users that their peers will identify for these assessed e-learning activities.

Instrument reliability is the ability of obtaining accurate, error-free results from the instrument used (Boudreau et al., 2001). Reliability was assessed using Cronbach's Alpha. Cronbach's Alpha is used to ensure test items are actually measuring the same construct (Jain, Ramamurthy, Hwa-Suk, & Yasai-Ardekani, 1998). Sekaran (2003) described Cronbach's Alpha as "a reliability coefficient that indicates how well the items in a set are positively correlated to one another" (p. 307). Although, Yoon, Guimaraes, and O'Neal (1995) stated a Cronbach's Alpha value above 0.50 to be acceptable in exploratory research, Sekaran (2003) noted reliabilities should be above 0.70 to be acceptable. Items that fall below a 0.70 factor be investigation further for instrument reliability.

External validity is "representativeness, or generalizability: to what populations, settings, and variables can this effect be generalized" (Campbell, 1957, p. 297). External validity requires that the findings of the results be generalized to beyond the people, setting or time when the study was conducted (Straub, 1989). The value and appropriateness of the use of students as research subjects in the use of IS research has been debated because of the 'settings' generalizability (Compeau, Marcolin, Kelley, & Higgins, 2012). Since the participants were taken from a single university, to improve generalizability, the student subjects used as a sample were only selected from a population of e-learning system users, thus, the findings in this study can be generalized to users of e-learning systems. Demographic information helped ensure that the data collected was a good representation of the sample and population (Compeau et al., 2012).

Population and Sample

This study included a sample population of only e-learners who had experience with e-learning systems and who could associate with the e-learning activities that were measured within the survey instrument. Sample population email addresses were obtained via approval of the Data Services Manager at a university in the northeastern US. Additionally, this study did not include e-learning course designers or instructors since the research goal was based on perceptions of end-users at the student level of e-learning activities. This restricted the population to e-learners only who were currently enrolled in online course(s). Although this approach narrowed the population, the nature of how e-learning is delivered via the Internet and the use of a university who actively offers e-learning on both a national and international geographic region allowed the response rate necessary to be analyzed.

Sheenhan (2001) completed a study that analyzed response rates for 31 Web-based studies using academic populations over a period of 15 years and found that the mean response rate was 36.83%. Response rates were increased when a pre-notification was sent within a short interval of time prior to the Web-based survey being solicited (Sheenhan, 2001). An advanced notification was sent to the e-learners one-week prior requesting them to participate in the Web-based survey. Kaplowitz, Hadlock, and Levine (2004) compared response rates of mail surveys along with Web-based surveys and found that response rates were comparable when an advanced notification was sent to the population. To increase response rates, an email was sent to the e-learners, which included an introduction to the purpose of this study and a Web link to the survey within Qualtrics. With a sample of over 15,000 enrolled e-learners, this study aimed to yield an

anticipated response rate of 5%. Appendix B contains a copy of the participation letter, which was sent one week prior to the Web link to the survey.

This study collected and analyzed data from a sample population, which targeted only e-learners from a single university in the US. All respondents received the same link to the Web-based survey instrument sent via e-mail. Web-based surveys are appropriate when used for populations that are familiar with the Internet (Sills & Song, 2002). Respondents were allowed to complete the Web-based survey assessment anonymously from any location, using any system that was convenient, and was not monitored during its completion. The duration of the survey did not exceed 30 minutes.

Pre-analysis Data Screening

To improve instrument validity and reliability, a pre-analysis data screening to detect problems with data collection was conducted (Levy, 2003). Mertler and Vannatta (2010) identified four main purposes for screening data prior to the main analysis that "will ultimately result in valid conclusions being drawn from the data" (p. 25). The first purpose aims to improve the accuracy of the data being collected in order to avoid inaccurate results, which lead to erroneous conclusions (Mertler & Vannatta, 2010). To ensure the analysis was accurate, the data was pre-screened for accuracy using descriptive statistics and frequency distributions to examine the data set (Levy, 2003; Mertler & Vannatta, 2010). Additionally, in this study, responses were collected directly through the Web-based survey, thus, reducing the opportunity for inaccurate data through transcription error or an inaccurate response value.

The second purpose is to check and remove the response-set, which happens when a participant responds to each test item using the same value (Levy, 2003). This study used

the pre-analysis data screening process outlined in Ferdousi and Levy (2010) to ensure

validity. After a visual inspection, any of the data items were eliminated where 100% of

the responses were submitted with the same score for all items (Ferdousi & Levy, 2010).

The third main purpose deals with missing or incomplete data. Sekaran (2003)

recommended the best way to improve validity is by attempting to reduce the possibility

of missing data via the collection process. In order to eliminate missing data, the option

within Qualtrics to require each response set to be completed in the survey prior to

submission was used.

 The fourth purpose deals with outliers, which are extreme cases that may skew results

(Mertler & Vannatta, 2010). The use of Mahalanobis Distance analysis identified

multivariate outliers that needed to be considered for removal. Mahalanobis Distance

analysis evaluates the distance of each record from the means of all the records using

Chi-Square statistics (Levy, 2006a).

Data Analysis

   RQ1a: What e-learning activities are perceived by users to have a high potential

     for threats of impersonation?

   RQ1b: What e-learning activities users perceived that their peers will identify to

     have a high potential for threats of impersonation?

   RQ2a: What levels of authentication strength are perceived by users to be most

     suitable against the threats of impersonation for these assessed e-learning

     activities?

RQ2b: What levels of authentication strength are perceived by users that their

peers will identify to be most suitable against the threats of impersonation

for these assessed e-learning activities?

The responses from the survey were analyzed using quantitative data analysis. Descriptive statistics was used to calculate the means and standard deviations for data collected for UP-HPI and PP-HPI (RQ1a & RQ1b) as well as UP-ASI and PP-ASI (RQ2a & RQ2b). The means were entered into a table format and sorted. The standard deviation, which represents the variability of the population, was reviewed to see how closely the responses were to the mean. A large standard deviation represents a high level of variability in response and was investigated further (Sekaran, 2003).

RQ1c: How do the e-learning activities perceived by users to have a high

potential for impersonation differ than what is perceived by users that

their peers will identify?

RQ2c: How do the levels of authentication strength perceived by users to be most

suitable against the threats of impersonation for these assessed e-learning

activities differ than what is perceived by users that their peers will

identify?

The mean results for UP-HPI and PP-HPI then for UP-ASI and PP-ASI were analyzed using a paired sample t-test to compare the calculated means to see if there were significant differences among the responses of the two groups. T-tests are used to determine if perceived differences between two groups are significantly different (Sekaran, 2003).This test aimed to determine how the perception of high potential for impersonation perceived by users and those users perceived that their peers would

identify differed between the groups and how the levels of authentication strength are

perceived as suitable against threats of impersonation for assessed e-learning activities

also differed between groups.

> *RQ3a:* *What are the significant components of the levels of authentication*
>
> *strength perceived by users to be most suitable against the threats of*
>
> *impersonation for these assessed e-learning activities?*
>
> *RQ3b:* *What are the significant components of the levels of authentication*
>
> *strength perceived by users that their peers will identify to be most*
>
> *suitable against the threats of impersonation for these assessed e-learning*
>
> *activities?*

Exploratory Factor Analysis (EFA) by using two separate Principal Component

Analysis (PCA) was used, one for RQ3a and another for RQ3b. Newsom (2005) stated

that "EFA is often recommended when researchers have no hypotheses about the nature

of the underlying factor structure of their measure" (p. 2). EFA has three basic decision

points: (1) decide the number of components, (2) choosing an extraction method, (3)

choosing a rotation method (Newsom, 2005).

PCA is widely used for exploratory and descriptive research (Mertler & Vannatta,

2010). PCA is used early in the research stage to consolidate numerous variables and to

consolidate the items and "describe and summarize data by grouping together variables

that are correlated" (Mertler & Vannatta, 2010, p. 343). Mertler and Vannatta (2010)

explained that PCA is considered an extraction method and uses four criteria for deciding

the appropriate number of components to retain. The first method uses eigenvalues and a

rule that components only with a value greater than one should be retained. The second

method retains components that account for 70% of the variability. The third method uses a graphical scree plot and retains all components along the sharp descent of the plot. The fourth method retains components only if residual value exceeds 0.05.

Cronbach's Alpha was used to analyze the consistency of responses items retained through PCA. "Cronbach's Alpha is a reliability coefficient that indicates how well the items in a set are positively correlated to one another" (Sekaran, 2003, p 307). Higher correlations of the response coefficients indicate that the response items are independent measures of the same concept (Sekaran, 2003). After the items had been explored from PCA and Cronbach's Alpha, any item that was deleted demonstrating low validity and reliability was further investigated for elimination from additional analysis.

> *RQ3c: What are the differences between the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities versus than what is perceived by users that their peers will identify?*

RQ3a and RQ3b may have resulted in a set of different significant components. Likewise, the responses retained through the PCA analysis of RQ3a and RQ3b may have differed among the two groups being analyzed. These differences were discussed based upon the varying components determined in EFA for RQ3a and RQ3b in RQ3c.

> *RQ4a: Are there significant differences of perception of high potential for threats of impersonation based on gender?*
>
> *RQ4b: Are there significant differences of perception of high potential for threats of impersonation based on age?*

RQ4c: Are there significant differences of perception of high potential for threats of impersonation based on e-learning experience?

The survey also collected data on demographic information for gender, age, and e-learning experience from each respondent. A frequency distribution and percentage was calculated for each demographic response for gender (RQ4a), age (RQ4b), and e-learning experience (RQ4c). Additionally, responses from RQ4a, RQ4b, and RQ4c were assessed against responses in RQ1a and RQ1b as well as RQ2a and RQ2b using an analysis of covariance (ANCOVA). ANCOVA is used when comparing means of two groups but with additional controls for a variable (covariant) that may influence the dependent variable (Mertler & Vannatta, 2010). This measured if there were any significant differences between the two groups based on demographic variables for each of the e-learning activities with high potential for impersonation along with their suitable levels of authentication strength.

Resource Requirements

In order to successfully complete this study the follow resources were used:

- Access to a pool of e-learners from a university in the US. The sample was collected from a population of students currently enrolled in online courses at a single university. This sample was accessible and approved for by the university's data services manager through the IRB process.

- Qualtrics: This Web-based survey tool was used to develop the survey instrument necessary to collect the data for this study. Most importantly this specific survey tool was used due to the unique two category format of the survey instrument. An

account was activated for use and the survey was designed to ensure the tool's successful implementation.

- Expert Panel: The pilot survey to validate the instrument relied on an expert panel of faculty colleagues and professionals in the IS field. Feedback from the expert panel was used to modify the survey instrument prior to collecting data from the targeted sample.

- Statistical Analysis Tool: SPSS was used to complete descriptive statistics, frequency distributions, Cronbach's Alpha, EFA, and PCA. Results were compiled and analyzed using lists and graphs available via the SPSS tool.

- Technology: The use of hardware, software, networking, and library resources was required in order to complete each step of the dissertation process. This technology was used for communications with advisor and committee, researching the literature, and writing the dissertation report. All necessary technology components were acquired.

Summary

Chapter three included a description of the research design, methodology, an explanation of the survey instrument, and measures that were used for this study. This study used an exploratory research design to develop an instrument to measure users' perceptions about suitable authentication methods for e-learning activities. The survey collected data on e-learning activities that were perceived by users and those perceived by users that their peers would identify to have high potential for impersonation. Additionally, the survey instrument collected relevant data on what levels of

authentication strength were perceived by users and those perceived by users that their peers would identify to be most suitable against the threats of impersonation for the assessed e-learning activities. A link to a Web-based survey was used to the solicit participation of e-learners to gather anonymous data on e-learning activities and authentication strength. The survey instrument is included in Appendix A of this dissertation.

Threats to validity and reliability along with procedures to mitigate them were discussed. Internal validity was addressed by using items from previously validated studies (Bailie & Jortberg, 2009; Levy, 2006b; Levy, 2008). Instrument validity was addressed by having an expert panel pre-screen the initial survey instrument to recommend adjustments prior to its delivery (Straub, 1989). Reliability removes weak measures by using criterion to select items closely related to the constructs (Moore & Benbasat, 1991). Cronbach's Alpha was used to ensure test items were actually measuring the same items and were reliable (Sekaran, 2003). A pre-analysis data screening process was discussed in order to improve instrument validity and reliability (Mertler & Vannatta, 2010). This section identifies how this study addressed the issues with reliability such as data that is inaccurate, response-set, missing, or outliers.

The data analyzed included the means of the responses for each e-learning activity and the selected authentication strength perceived suitable to secure the e-learning activity from impersonation fraud. This data was analyzed using descriptive statistics such as sorting of the means and standard deviations. Further, a paired sample t-test for means checked the data for statistical significant differences between the users and those perceived by users that their peers would identify for both e-learning activities and

authentication strength. Finally, a list of resource requirements was included that was necessary for the successful implementation of this study.

Chapter 4

Results

Overview

This chapter outlines results of the data analysis for this empirical study. The results for this study were completed in three phases. Each phase is detailed in this section in the order it was conducted. Phase one details the development of a new Web-based survey instrument based upon a thorough literature review used in exploratory studies within IS (Boudreau et al., 2001).

Phase two details the adjustments to the Web-based survey instrument using the Delphi method, which gathered expert panel feedback (Okoli & Pawlowski, 2004). Phase three contains subsections detailing the steps involved in data collection and analysis. The pre-analysis data screening subsection discusses the results of the review of the raw data for accuracy, response-set, missing data, and outliers (Levy, 2003). The descriptive statistics subsection discusses the data analysis along with results for RQ1a, RQ1b, RQ2a, and RQ2b. Also in that subsection are the results of the paired sample t-test for means that was performed for RQ1c and RQ2c. The exploratory factor analysis subsection contains the results and discussions from the PCA analysis and Cronbach's Alpha reliability test. The final subsection includes the significance test for differences on the demographic variables.

Exploratory Research (Phase One)

For phase one, a survey instrument was developed based on existing measures in order to collect data for this study. An extensive literature review was conducted in the IS and Web-based systems literature in order to identify the CVFs of e-learning systems and demographic variables of e-learning system users. The survey instrument was developed using e-learning activity items adapted from prior studies with the highest CVF rankings (Bailie & Jortbert, 2009; Levy, 2006b; & Levy, 2008). The demographic variables on the survey instrument were selected based on prior studies that found that gender, age, and e-learning experience had a significant influence in IS misuse (Lanier, 2006). The survey instrument was designed electronically using Qualtrics, a Web-based survey tool.

Delphi Method (Phase Two)

Using the Delphi method outlined in Okoli and Pawlowski (2004), after the initial development of the Web-based survey instrument, an expert panel was organized to conduct a pre-screening of the instrument and recommend any changes to the list of e-learning activities due to vague or missing items and to the validate the authentication scale with regards to strength. The Delphi panel consisted of 10 experts from the IS field. Table 12 lists the number of experts used on the panel from the areas of IS.

Table 12. Delphi Panel Experts

Area of Expertise	Number of Experts
IS Academic Department	4
Information Security	2
Authentication Methods	2
E-learning Providers	2

Feedback was gathered from the expert panel, interpreted, and an initial round of adjustments was made to the survey instrument. Table 13 lists the collective feedback from all experts and the adjustments made to the instrument.

Table 13. Delphi Expert Panel Suggested Adjustments to Initial Survey Instrument

Change #	Feedback	Adjustments
1.	The use of coding values (UP-HPI, PP-HPI, UP-ASI, PP-ASI) on the survey sections A & B were confusing.	Coding values were changed to simply "U" for user and "P" for peer on the Web portion of the survey, which was seen by participants. The coding values "UA", "PA", "UB", and "PB" were assigned to the items relative to section A and B used for analysis only.
2.	Items using the verbiage such as "official" or "unofficial" are vague and misleading.	The verbiage "official" and "unofficial" was changed to a specific activity description such as "post", "submit", or "reply".
3.	Section B needs definitions for the types of authentication.	Definitions for each type of authentication being evaluated within the survey were provided.

Any additions or removal of items would have been done at this time, however, none of the 18 e-learning activities items were asked to be removed, and no new ones were requested to be added. The expert panel was asked to repeat the review process again on the revised instrument to validate the interpretation of the original feedback and adjustments. No further suggestions were given on the survey instrument, thus, no additional iterations with the experts were required, given all reached a consensus on the adjusted instrument. The Delphi method increased the validity of the instrument to ensure the validity of the authentication scale and selection of the e-learning activities.

Quantitative Research (Phase Three)

Pre-Analysis Data Screening

In phase three, a participation letter and a link to the Web-based survey was emailed

to over 15,000 e-learners through Qualtrics. Out of the 15,000 invitations to participate,

1,086 responses were collected, generating a 7.2% response rate. The survey instrument

required that all responses be answered prior to submitting the completed survey, thereby

ensuring no missing data was possible. Since the response items were given using a

multiple-choice Likert-scale and contained no open-ended questions, this forced users to

select from the preset scale of values to ensure data accuracy. The data set containing all

the completed responses were downloaded and imported into Statistical Package for the

Social Sciences (SPSS) for further pre-analysis data screening. The data set was analyzed

for any response-set issues, where participants responded by selecting the same scale

value to all the e-learning activities being assessed (Levy, 2003). After a visual

inspection, nine (less than 1%) cases were response-set answers. The response-set cases

were removed from the data set leaving 1,077 remaining useful cases. Responses from

any participant who selected they had no e-learning experience would have been removed

since the assumption was that participates had at least one course of e-learning

experience; however, no respondents selected "none" for e-learning experience so no

further cases needed to be removed.

Respondents were forced to select from a fixed Likert-scale and were unable to leave

any items unanswered. However, to ensure the accuracy of the data, descriptive statistics

were used to identify the minimum and maximum value for each item to determine if

responses were within the expected value range and were not accidently corrupted during

the transfer of data between Qualtrics and SPSS. All responses were within the expected ranges and none were removed.

The final step for pre-analysis data screening was to identify multivariate outliers by completing a Mahalanobis Distance analysis within SPSS on the survey items. A 95% confidence level was used in order to identify multivariate outliers. Seven outlier cases were removed from the data set due to multivariate outliners, leaving 1,070 useful cases in total for further data analysis. Appendix A contains a copy of the revised final survey instrument used to collect the data.

Descriptive Statistics Data Analysis

To answer RQ1a the useful cases were analyzed by using descriptive statistics to calculate the means and standard deviations for e-learning activities perceived by users to have a high potential for threats of impersonation (UP-HPI). The means were sorted from lowest to highest perceived potential for threat of impersonation. The results were separated into two groups: (a) agree – all e-learning activities that have a mean below 3.0; and (b) disagree – all e-learning activities that have a mean of 3.0 or higher. Table 14 contains the sorted means of the 18 e-learning activities surveyed for UP-HPI.

Table 14. Descriptive Statistics for UP-HPI (Means and Standard Deviations) (N=1,070)

Item	Mean	Standard Deviation
UA16	2.33	.948
UA15	2.34	.927
UA14	2.36	.907
UA18	2.40	.817
UA2	3.15	1.182
UA3	3.23	1.152
UA8	3.27	1.283
UA7	3.43	1.160
UA9	3.43	1.213
UA6	3.43	1.145
UA1	5.06	1.270

Table 14. Descriptive Statistics for UP-HPI (Means and Standard Deviations) (continued) (N=1,070)

Item	Mean	Standard Deviation
UA12	5.13	1.665
UA13	5.13	1.667
UA5	5.20	1.361
UA4	5.25	1.350
UA11	5.35	1.608
UA10	5.36	1.612
UA17	5.99	1.041

Figure 10 depicts the two groups, which shows a clear distinction between the e-learning activities with a perceived high potential for impersonation as opposed to those that do not. The four e-learning activities that had a mean below 3.0 indicating they have a high potential for impersonation were: UA16 'Submit quizzes online', UA15 'Submit exams online', UA14 'Submit assignments online', and UA18 'Submit projects online', which are considered high-stakes summative assessments.
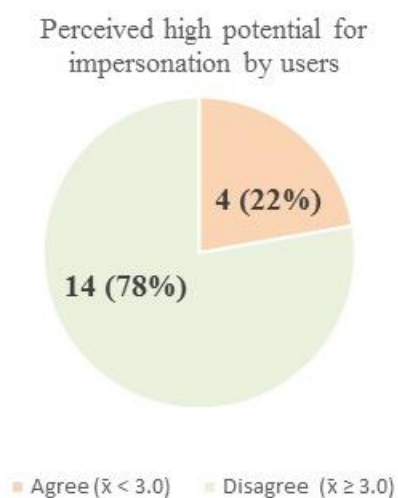
Figure 10. Grouped Means for UP-HPI (N=1,070)

RQ1b was answered in a similar fashion by using descriptive statistics to calculate the means and standard deviations for e-learning activities users perceived that their peers would identify to have a high potential for threats of impersonation (PP-HPI). The means were sorted from lowest to highest perceived potential of threat of impersonation. The results were separated into two groups: (a) agree – all e-learning activities that have a mean below 3.0; and (b) disagree – all e-learning activities that have a mean of 3.0 or higher. Table 15 contains the sorted means of the 18 e-learning activities items for PP-HPI.

Table 15. Descriptive Statistics for PP-HPI (Means and Standard Deviations) (N=1,070)

Item	Mean	Standard Deviation
PA15	2.32	.924
PA14	2.33	.905
PA16	2.33	.925
PA18	2.40	.823
PA2	2.96	1.253
PA8	3.01	1.351
PA6	3.18	1.293
PA3	3.18	1.174
PA9	3.41	1.223
PA7	3.42	1.183
PA1	5.06	1.384
PA13	5.10	1.665
PA12	5.10	1.671
PA5	5.17	1.376
PA4	5.20	1.402
PA10	5.30	1.636
PA11	5.33	1.624
PA17	5.86	.999

Figure 11 depicts the two groups that similarly to UP-HPI, which shows a clear distinction between the e-learning activities with a perceived high potential for impersonation as opposed to those that do not. The five e-learning activities that had a mean below 3.0 and a high potential for impersonation were: PA15 'Submit exams

online', PA14 'Submit assignments online', PA16 'Submit quizzes online', and PA18 'Submit projects online', which are considered high-stakes summative assessments, but also included PA2 'Participate in text-chat sessions with the professor', which is considered a formative assessment.

Perceived high potential for impersonation
that users think their peers will identify

5 (28%)

13 (72%)

■ Agree (x̄ < 3.0)   ■ Disagree (x̄ ≥ 3.0)
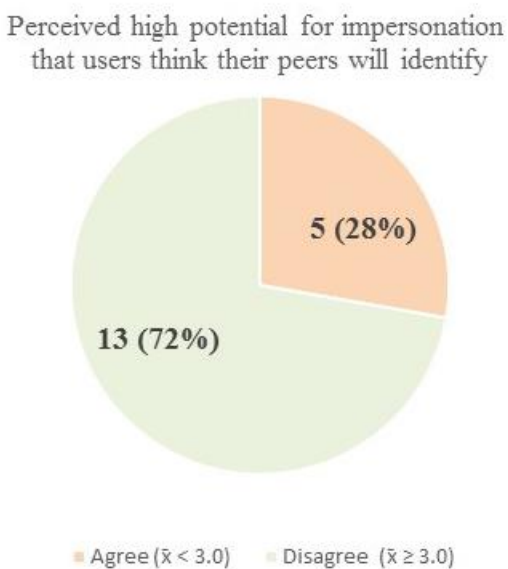
Figure 11. Grouped Means for PP-HPI (N=1,070)

These results indicate that e-learners do perceive a higher risk of impersonation for e-learning activities that are primarily categorized as summative or as high-risks e-assessment. In order to better secure the e-learning system, e-learning providers would be interested in these results to know which e-learning activities users are more likely to allow for deliberate impersonation. Although, there was the addition of the fifth e-learning activity (PA2) in PP-HPI, the mean was very close to "neither agree or disagree" and also had the largest standard deviation out of the list of items. Thus, the inclusion of PA2 does not seem to create a variation in the perceived e-learning activities that are most susceptible to impersonation between the two sets of responses. The four

top e-learning activities support the study by Apampa et al. (2010) that impersonation fraud is a major threat to summative e-assessments. Therefore, the first goal of this study to determine what e-learning activities are perceived by users to have a high potential for threats of impersonation (1a) and what e-learning activities user perceived that their peers would identify to have a high potential for threats of impersonation (1b) have been determined.

To answer RQ1c, the means and standard deviations results for each group, UP-HPI and PP-HPI, were compared using a paired sample t-test to determine if there were significant differences between the two groups as it relates to perceived threat of impersonation for selected e-learning activities. The results of the paired sample t-test indicated that 12 out of 18 activities had means that were significantly different between the groups. The results of the paired sample for means t-test are presented in Table 16 and Figure 12.

Table 16. Mean Scores, Standard Deviation, and Paired Sample Results for UP-HPI & PP-HPI (N=1,070)

Item	UP-HPI Mean	UP-HPI SD	PP-HPI Mean	PP-HPI SD	Paired Means t	Paired Means Sig.	
1	5.06	1.270	5.06	1.384	.052	.9584	
2	3.15	1.182	2.96	1.253	13.727	**.0000**	***
3	3.23	1.152	3.18	1.174	1.427	.1539	
4	5.25	1.350	5.20	1.402	5.097	**.0000**	***
5	5.20	1.361	5.17	1.376	3.459	**.0006**	***
6	3.43	1.145	3.18	1.293	7.240	**.0000**	***
7	3.43	1.160	3.42	1.183	.466	.6413	
8	3.27	1.283	3.01	1.351	7.190	**.0000**	***
9	3.43	1.213	3.41	1.223	1.765	.0779	
10	5.36	1.612	5.30	1.636	5.537	**.0000**	***
11	5.35	1.608	5.33	1.624	1.964	**.0498**	*
12	5.13	1.665	5.10	1.671	2.813	**.0050**	**
13	5.13	1.667	5.10	1.665	4.028	**.0001**	***

Table 16. Mean Scores, Standard Deviation, and Paired Sample Results for UP-HPI & PP-HPI (N=1,070) (continued)

Item	UP-HPI Mean	SD	PP-HPI Mean	SD	Paired Means t	Sig.	
14	2.36	.907	2.33	.905	4.065	.0001	***
15	2.34	.927	2.32	.924	3.732	.0002	***
16	2.33	.948	2.33	.925	0.000	1.0000	
17	5.99	1.041	5.86	.999	11.959	.0000	***
18	2.40	.817	2.40	.823	.277	.7817	

*** p < 0.001, ** p < 0.01, * p < 0.05
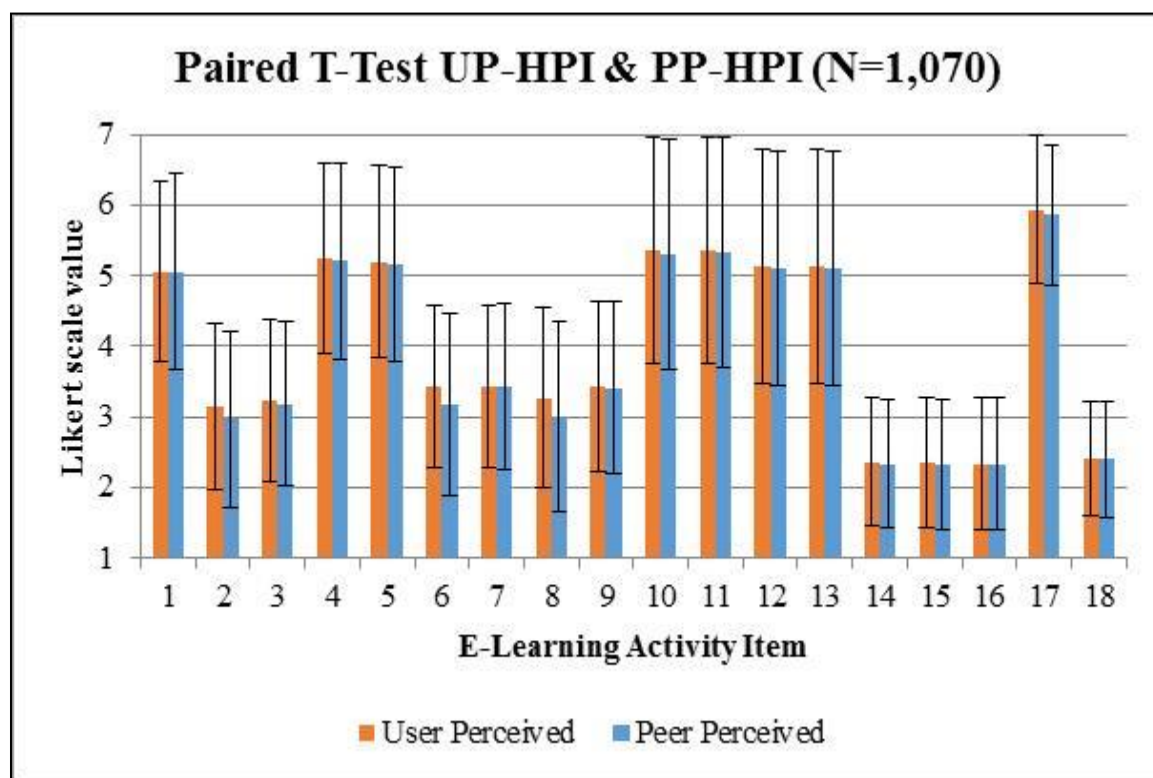
Figure 12. Paired T-Test for UP-HPI & PP-HPI (N=1,070)

In each instance the PP-HPI mean response for the threat of impersonation was higher than the UP-HPI response mean. Although, this study did not directly ask the respond if the respondents allowed themselves to be deliberately impersonated, this supports that

studies that found that self-reported results are often under-reported (Gibson et al., 2008).
A point of interest, however, is although there were significant differences in the means
for more than half the e-learning activities being measured, the same four activities were
identified for both UP-HPI and PP-HPI as having the perceived highest threat of
impersonation overall.

To answer RQ2a the useful cases were analyzed by using descriptive statistics to
calculate the means and standard deviations for levels of authentication strength
perceived by users to be most suitable against the threat of impersonation for assessed
e-learning activities (UP-ASI). The means were sorted from highest to lowest level of
authentication strength. The results were separated into three groups: (a) High Strength
including Live-proctor – all e-learning activities that have a mean of 5.0 and above; (b)
Low-Moderate strength including Biometric – all e-learning activities that have a mean of
2.5 and above but below 5.0; (c) Very low strength – all e-learning activities that have a
mean below 2.5. Table 17 contains the sorted means of the 18 e-learning activities
surveyed for UP-ASI.

Table 17. Descriptive Statistics for UP-ASI (Means and Standard Deviations) (N=1,070)

Item	Mean	Standard Deviation
UB15	5.43	1.265
UB16	5.36	1.252
UB18	3.25	1.093
UB14	2.80	.992
UB2	2.60	.868
UB11	2.05	1.116
UB10	2.02	1.108
UB3	1.85	1.078
UB4	1.62	1.111
UB5	1.59	1.067
UB13	1.57	.974
UB12	1.55	.962

Table 17. Descriptive Statistics for UP-ASI (Means and Standard Deviations) (N=1,070) (continued)

Item	Mean	Standard Deviation
UB1	1.54	.925
UB8	1.37	.831
UB7	1.35	.817
UB6	1.32	.799
UB9	1.23	.653
UB17	1.10	.442

Figure 13 depicts the three groups, which shows a clear distinction between the levels of authentication strength suitable for assessed e-learning activities. The two e-learning activities that had a mean of 5.0 and above were: UB15 'Submit exams online' and UB16 'Submit quizzes online'. These were identified as needing a strong authentication factor that uses live-proctor authentication along with at least one other factor such as a password or biometric in order to reduce the threat of impersonation. The second group had three e-learning activities that had a mean of 2.5 and above but below 5.0, which included UB18 'Submit projects online', UB14 'Submit assignments online', and UB2 'Participate in text-chat sessions with the professor'. It is noteworthy to point out that these are the same high-stakes summative assessments that were identified as having the highest potential for impersonation for UP-HPI.

Level of authentication strength perceived by users
most suitable for assessed e-learning activities

2, 11%

3, 17%

13, 72%

■ High Strength (x̄ ≥ 5.0)   ■ Moderate - Low Strength (x̄ ≥ 2.5 and x̄ < 5.0)   ■ Very Low Strength (x̄ < 2.5)
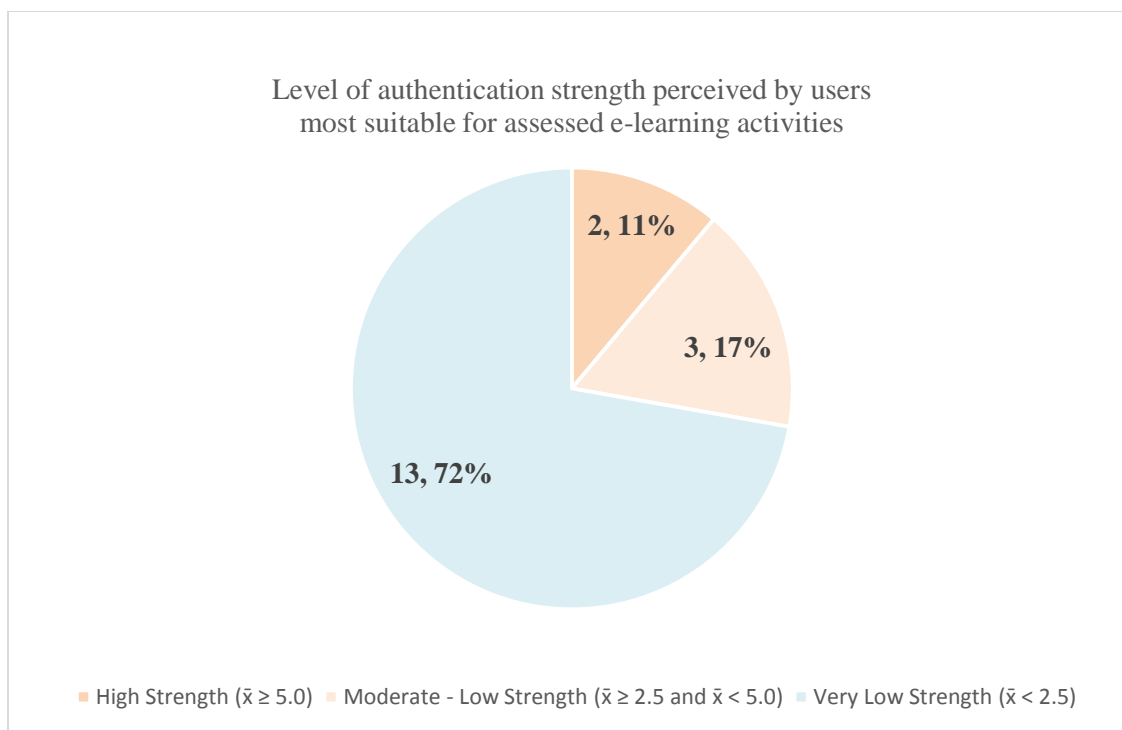
Figure 13. Grouped Means for UP-ASI (N=1,070)

Research question 2b was answered in a similar fashion by using descriptive statistics

to calculate the means and standard deviations for levels of authentication users perceived

that their peers will identify as most suitable e-learning activities against the threat of

impersonation (PP-ASI). The means were sorted from highest to lowest level of

authentication strength. The results were separated into three groups: (a) High Strength

including Live-proctor – all e-learning activities that have a mean of 5.0 and above; (b)

Low-Moderate strength including Biometric – all e-learning activities that have a mean of

2.5 and above but below 5.0; (c) Very low strength – all e-learning activities that have a

mean below 2.5. Table 18 contains the sorted means of the 18 e-learning activities

surveyed for PP-ASI.

Table 18. Descriptive Statistics for PP-ASI (Means and Standard Deviations (N=1,070)

Items	Mean	Standard Deviation
PB15	5.43	1.253
PB16	5.36	1.253
PB18	3.27	1.109
PB14	2.80	1.009
PB2	2.57	.875
PB11	2.06	1.122
PB10	2.05	1.116
PB3	1.83	1.070
PB4	1.62	1.104
PB5	1.60	1.066
PB13	1.59	.987
PB12	1.58	.974
PB1	1.55	.939
PB8	1.40	.854
PB7	1.37	.849
PB6	1.34	.815
PB9	1.28	.711
PB17	1.11	.463

Figure 14 depicts the three groups, which shows a clear distinction between the levels of authentication strength suitable for assessed e-learning activities. The two e-learning activities that had a mean of 5.0 and above were: UB15 'Submit exams online' and UB16 'Submit quizzes online'. These were identified as needing a strong authentication factor that uses live-proctor authentication along with at least one other factor such as a password or biometric in order to reduce the threat of impersonation. The second group had three e-learning activities that had a mean of 2.5 and above but below 5.0, which included UB18 'Submit projects online', UB14 'Submit assignments online', and UB2 'Participate in text-chat sessions with the professor'. Again, it is noteworthy to point out that these are the same high-stakes summative assessments that were identified as having the highest potential for impersonation for PP-HPI.

Level of authentication strength perceived by users that their peers will identify as most suitable for assessed e-learning activities

2, 11%

3, 17%

13, 72%

■ High Strength (x̄ ≥ 5.0) ■ Moderate - Low Strength (x̄ ≥ 2.5 and x̄ < 5.0) ■ Very Low Strength (x̄ < 2.5)
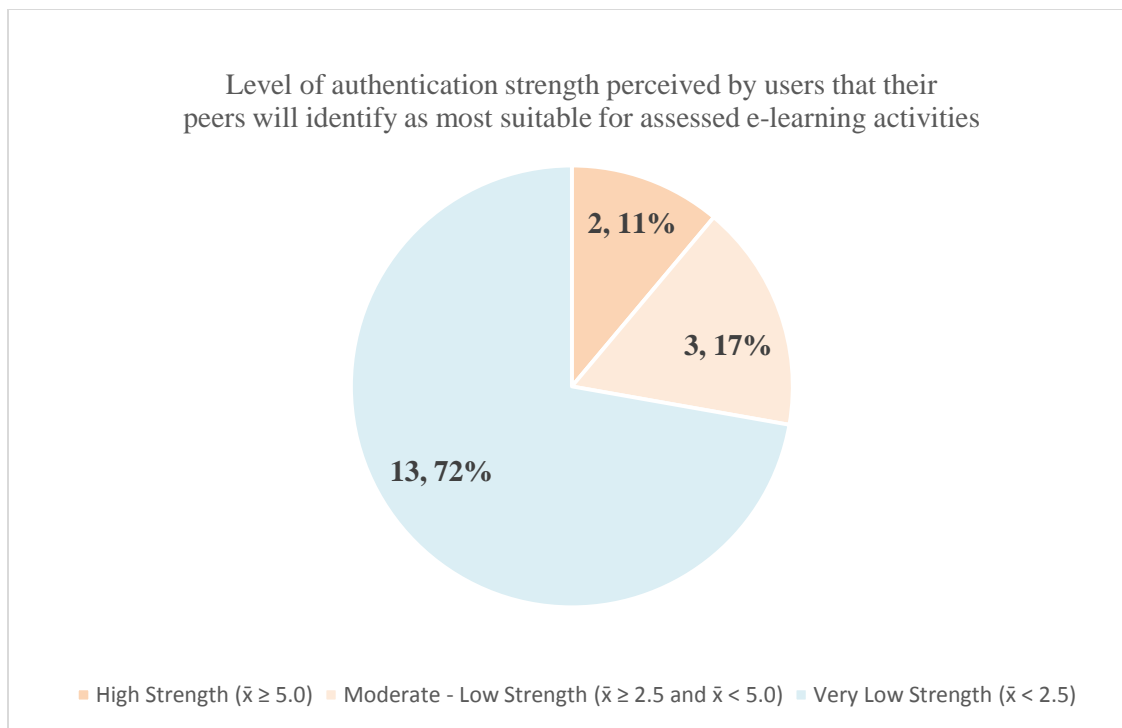
Figure 14. Grouped Means for PP-ASI (N=1,070)

These results indicate that e-learners do perceive that suitable levels of authentication must vary in strength based upon the activity being considered. The five e-learning activities that were identified as having the highest potential of threat of impersonation were primarily categorized as summative or as high-risks e-assessment. They were perceived to need a stronger authentication method other than a single-factor authentication username/password that is used to authenticate users at the system level. In order to better secure the e-learning system at the activity level, e-learning providers would be interested in these results to know which e-learning activities are perceived to need a suitable level authentication other than a 'one size fits all' username/password system approach to reduce the risk of deliberate impersonation (Helkala & Snekkenes, 2009). Therefore, the second goal of this study was to determine what levels of

authentication strength are perceived by users and by users that their peers would identify

to be most suitable against the threats of impersonation have provided findings that

support that a 'one size fits all' approach to authentication is not suitable for all

e-learning activities. There is a perception that summative e-assessments need a stronger

authentication method, which includes at least a biometric and upward to a live-proctor

authentication.

To answer RQ2c, the means and standard deviations results for each group, UP-ASI

and PP-ASI, were compared using a paired sample t-test to see if there were significant

differences between the two groups as it relates to levels of authentication strength for

assessed e-learning activities. The results of the paired sample t-test indicated that 9 out

of 18 activities had means that were significantly different between the groups. The

results of the paired sample t-test for means are presented in Table 19 and Figure 15.

Table 19. Mean Scores, Standard Deviation, and Paired Sample Results for UP-ASI &
PP-ASI (N=1,070)

Item	UP-ASI Mean	SD	PP-ASI Mean	SD	Paired Means t	Sig.	*
1	1.54	.925	1.55	.939	-1.859	.0633	
2	2.60	.868	2.57	.875	2.441	**.0148**	*
3	1.85	1.078	1.83	1.070	2.226	**.0262**	*
4	1.62	1.111	1.62	1.104	0.000	1.0000	
5	1.59	1.067	1.60	1.066	-1.874	.0612	
6	1.32	.799	1.34	.815	-2.021	**.0435**	*
7	1.35	.817	1.37	.849	-3.414	**.0007**	***
8	1.37	.831	1.40	.854	-3.482	**.0005**	***
9	1.23	.653	1.28	.711	-3.871	**.0001**	***
10	2.02	1.108	2.05	1.116	-2.808	**.0051**	**
11	2.05	1.116	2.06	1.122	-1.521	.1284	
12	1.55	.962	1.58	.974	-2.460	**.0140**	*

Table 19. Mean Scores, Standard Deviation, and Paired Sample Results for UP-ASI &
PP-ASI (N=1,070) (continued)

	UP-ASI		PP-ASI		Paired Means		
Item	Mean	SD	Mean	SD	t	Sig.	*
13	1.57	.974	1.59	.987	-1.238	.2161	
14	2.80	.992	2.80	1.009	-.194	.8461	
15	5.43	1.265	5.43	1.253	-.988	.3234	
16	5.36	1.252	5.36	1.253	.738	.4604	
17	1.10	.442	1.11	.463	-1.213	.2254	
18	3.25	1.093	3.27	1.109	-2.324	**.0203**	*

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$
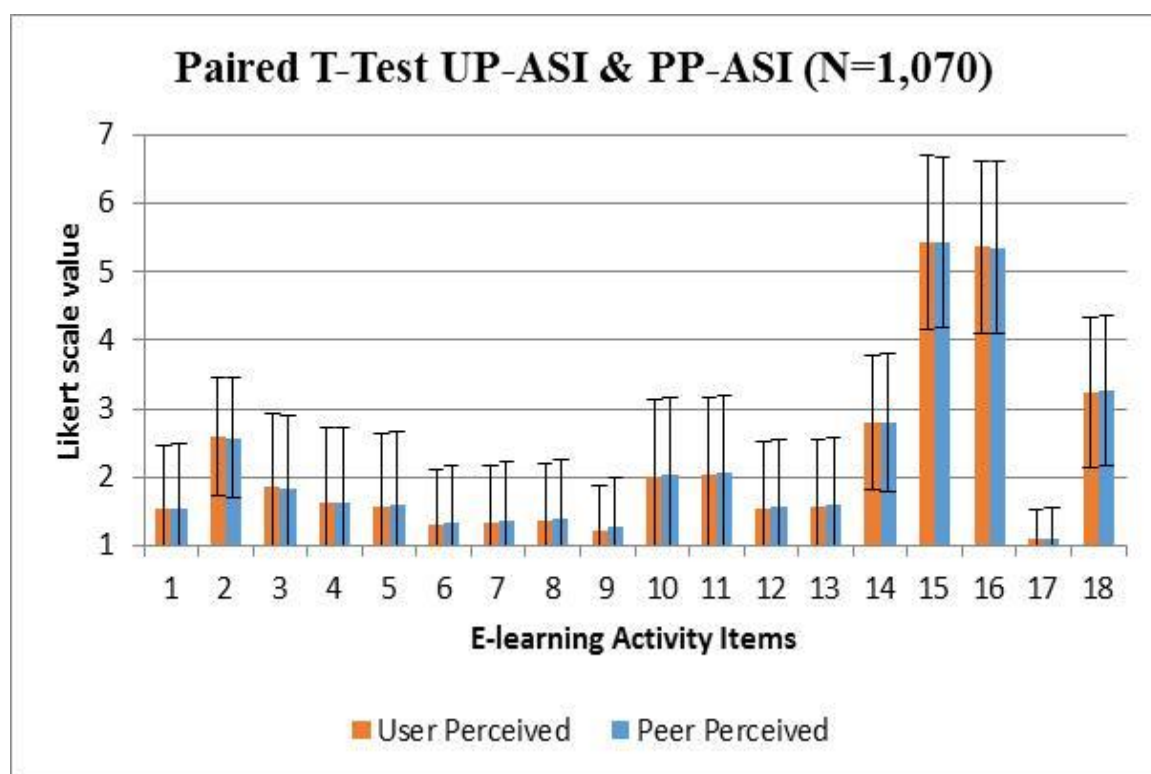
Figure 15. Paired T-Test for UP-ASI & PP-ASI (N=1,070)

Nine out of 18 items had a significant difference in means. Unlike the consistent

findings within RQ1c, RQ2c had a variation regarding which mean was greater between

the two groups. The only two activities that were significant based upon the responses

from RQ2a and RQ2b were item 2 'Participate in text-chat sessions with the professor'

and item 18 'Submit projects online'. Item 2 had indicated a stronger authentication in

the UP-ASI group, whereas, item 18 had indicated a stronger authentication in the

PP-ASI group. For the other three items identified in RQ2a and RQ2b there was no

significant differences indicating that users believed their peers would perceive the same

level of authentication strength is necessary for those summative e-assessments.

Exploratory Factor Analysis by Principal Component Analysis

The significant components of the levels of authentication strength perceived by users

and those users perceived that their peers would identify to be most suitable against the

threats of impersonation for assessed e-learning activities were identifying using EFA via

PCA as an extraction method with Varimax rotation. Mertler and Vannatta (2010)

outlined four criteria for deciding the appropriate number of components. The first and

second criteria state that eigenvalues greater than one should be retained for components

that make up at least 70% variability. Any components with eigenvalues less than one

should be considered for deletion. Additionally, components are only retained if the

factor loading exceeds .5. Finally, a scree plot is a graphical representation of the retained

components with the highest magnitude at the top leading to a decline to successive

Eigenvalues (Mertler & Vannatta, 2010).

The literature review identified top e-learning activities based on CVFs (Levy, 2008).

The activities where defined into two main overarching categories of formative e-

assessments and summative e-assessments (Apampa et al., 2010). Furthermore, the main

categories were divided into subcategories adapted from other studies: Instructional,

Collaborative, Practice, and Assessments (Bailie & Jortberg, 2009; Fry, 2001; Levy,

2008). PCA was used against the 18 e-learning activities and the subcategories were used

to describe the retain components. To answer the RQ3a and RQ3b, seven significant components sets were retained and 4 individual components were identified.

The initial PCA analysis for RQ3a suggested eight components. The items were examined for low loadings ($< .4$) and for medium loading ($.4 \geq$ to $< .6$) on more than one factor. The results of this initial review discovered that item 14 and item 18 did not load well within their component group because of negative or very low load values, respectively. In an attempt to make item 14 and item 18 load with all the other items, another analysis was completed forcing the components to fit to seven components. Sixteen of the 18 items were grouped similarly, however, the variability accountability went down to 77% and item 14 and item 18 were still not loading well within their group.

An investigation of item 14 (submitting assignments online) and item 18 (submitting projects online) revealed that although both were identified as having a high potential for impersonation, the literature has some contradictions in terms of how these items are categorized. For example, Fry (2001) categorized both items as formative, low-stakes e-assessments, whereas, Levy (2008) categorized both items as formal, summative e-assessments. In contrast, the other 16 items were consistently categorized as collaborative (or communication, informal), practice (ungraded, informal) or assessment (formal, summative) in the literature. This investigation explains why item 14 and item 18 are susceptible to various interpretations in terms of authentication. Following this conclusion and based on the low loadings values item 14 and item 18, it was determined that removing the items from the analysis provided the best loading of items retained. After the items were removed, a final PCA analysis was completed resulting in an acceptable component to retain. The retained items within the eight components had

eigenvalues greater than one, accounted for 83% of the variability, and all retained

components had a factor loading of at least 0.58.

   A Cronbach's Alpha analysis on all components was completed to review reliability

of the retained components. The components with a Cronbach's Alpha of 0.70 or higher

were; Collaborative: Voice Chat - 0.965; Practice: Share Assignments - 0.966;

Assessment: Quizzes & Exams-0.966; Collaborative: Sending E-mail - 0.961 indicating a

very high reliability. These components explained the greatest amount of variability and

there was a consensus in the literature in terms of how these items were categorized.

Therefore, these components represent the types of activities that e-learners were most

familiar and understood not only the potential for threat of impersonation but also the

most suitable level of authentication strength necessary to reduce that threat. Two

components had a moderate Cronbach's Alpha of $0.50 \geq$ or < 0.75: Collaborative:

Discussion Post - 0.739 and Collaborative: Discussion Reply - 0.656. Yoon et al., (1995)

stated that in exploratory research values 0.50 and above were acceptable. Due to the

nature of this exploratory research components 5 and 6 are considered reliable in terms as

being collaborative, however, it is understandable that since collaborative activities can

be subcategorized as a formative or summative activity, the interpretation may be vague

and need to be further description. Component 7 had a low Cronbach's Alpha of < 0.50:

Collaborative: Text-Chat - 0.408. Items in this component were consistently categorized

in the literature as collaborative informal text-chat activities. The eighth component had

an extremely low Cronbach's Alpha of 0.057 and subsequently removed from the

component analysis. This removed component often represents ungraded or informal

activities such as practice quizzes or setting up online profile and was identified as highly

unlikely to be susceptible to impersonation. The PCA resulted in seven component sets

and four individual items (submit assignments, submit projects, develop a personal

Website, profile, or blog, and ungraded quizzes). The results of the PCA and Cronbach's

Alpha analysis for RQ3a are shown in Figure 16.

Significant Components Retained from PCA for UP-ASI								
Item	**Factor**	**Rotated Component Matrix**						
		1	**2**	**3**	**4**	**5**	**6**	**7**
4	**Collaborative:** Voice Chat	.967						
5		.963						
13	**Practice:** Share Assignments		.982					
12			.981					
15	**Assessment:** Quizzes & Exams			.983				
16				.982				
11	**Collaborative:** Sending E-mail				.980			
10					.978			
6	**Collaborative:** Discussion Post					.899		
7						.872		
9	**Collaborative:** Discussion Reply						.851	
8							.851	
3	**Collaborative:** Text-Chat							.831
2								.607
Cronbach's Alpha		0.965	0.966	0.966	0.961	0.739	0.656	0.408

Figure 16. Significant Components Retained from PCA for UP-ASI (N=1,070)

The initial PCA analysis for RQ3b suggested the same seven components as RQ3a.

The items were examined for low loadings ($< .4$) and for medium loading ($.4 \geq$ to $< .6$)

for more than one factor. The results of this initial review discovered that the same two

items, item 14 and item 18, did not load well within their component group because of

negative load values. Because these results were nearly mirror the first PCA, no further

analysis was done. Using the same conclusion for item 14 and 18 as in the first PCA and based on the low loadings values item 14 and item 18, it was determined that removing the items from the analysis provided the best loading of items retained. After the items were removed, a final PCA analysis was completed resulting in acceptable components. The retained items within the seven components had eigenvalues greater than one, accounted for 82% of the variability and all retained components had a factor loading of at least 0.69. Likewise, the same four individual items (submit assignments, submit projects, develop a personal Website, profile, or blog, and ungraded quizzes) were identified.

A Cronbach's Alpha analysis on all components was completed to review reliability of the retained components. The components with a Cronbach's Alpha of 0.70 or higher were; Collaborative: Voice Chat - 0.932; Practice: Share Assignments - 0.937; Assessment: Quizzes & Exams-0.928; Collaborative: Sending E-mail - 0.912 and Discussion Post - 0.806 indicating a very high reliability. These components explained the greatest amount of variability and there was a consensus in the literature in terms of how these items are categorized. Therefore, these components represent the types of activities that e-learners are most familiar and understood not only the potential for threat of impersonation but also the most suitable level of authentication strength necessary to reduce that threat. One component had a moderate Cronbach's Alpha of $0.50 \geq$ or < 0.70: Collaborative: Discussion Reply - 0.682. The last component 7 again, had a low Cronbach's Alpha of < 0.50: Collaborative: Text-Chat - 0.379. The results of the PCA and Cronbach's Alpha analysis for RQ3b are shown in Figure 17.

		Rotated Component Matrix						
Item	**Factor**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
4	**Collaborative:** Voice Chat	.953						
5		.950						
15	**Assessment:** Quizzes & Exams		.969					
16			.968					
13	**Practice:** Share Assignments			.964				
12				.963				
11	**Collaborative:** Sending E-mail				.959			
10					.956			
9	**Collaborative:** Discussion Post					.914		
8						.907		
6	**Collaborative:** Discussion Reply						.888	
7							.847	
3	**Collaborative:** Text-Chat							.872
2								.602
Cronbach's Alpha		0.932	0.937	0.928	0.912	0.806	0.682	0.379

Figure 17. Significant Components Retained from PCA for PP-ASI (N=1,070)

Upon completion of the two PCA analyses, seven categories comprised of 14 items were retained. Table 20 lists the items along with their categories and activity definition. The results of this analysis answer the research questions: RQ3a *'What are the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities?'* and RQ3b: *'What are the significant components of the levels of authentication strength perceived by users that their peers will identify to be most suitable against the threats of impersonation for these assessed e-learning activities?'.*

Table 20. List of Reliable E-learning Activities Grouped by Category

Item	Category	E-learning Activity
2	**Collaborative:** Text-Chat	Participate in text-chat sessions with the professor
3		Participate in text-chat sessions with other students
4	**Collaborative:** Voice-Chat	Participate in live voice-chat sessions with the professor
5		Participate in live voice-chat sessions with other students
6	**Collaborative:** Discussion Reply	Post in new discussion forum message with to the professor
7		Post in new discussion forum message with other students
8	**Collaborative:** Discussion Post	Reply to discussion forum messages to the professor
9		Reply to discussion forum messages with other students
10	**Collaborative:** Sending E-mail	Send e-mails to other students
11		Send e-mails to the professor
12	**Practice:** Share Assignments	Share assignments with other students (via discussion forum)
13		Share assignments with other students (via e-mail)
15	**Assessment:** Quizzes & Exams	Submit exams online
16		Submit quizzes online

The third goal of this study sought to identify the differences between the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation perceived by users and those that their peers would identify. After completing two PCA analyses, one for each group, it was determined that there are no differences between the significant components. In fact, the factor loadings and the Cronbach's Alpha were very consistent among the two groups. This demonstrated a high reliability in the results for the level of authentication most suitable for the 18 e-learning activities. For the four items that were not retained either because of

low factor loading or low Cronbach's Alpha values, more investigation is necessary to describe the e-learning activity or identify the formative or summative categories.

Demographic Data Analysis

Demographic data collected from the 1,070 e-learners included gender, age, and e-learning experience. The demographic analysis conducted in SPSS included a frequency distribution and percentage rate for each item. Table 21 shows the demographic distribution of the results of the 1,070 respondents.

Table 21. Descriptive Statistics of Population (N=1,070)

Item	Frequency	Percentage (%)
Gender		
Male	445	41.6
Female	625	58.4
Age		
Under 20	51	4.8
20 - 29	344	32.1
30 - 39	291	27.2
40 - 49	326	30.5
50 - 59	27	2.5
60 or over	31	2.9
E-learning Experience (in # online courses)		
1 - 5	484	45.2
6 - 10	472	44.1
11+	114	10.7

The rate of responses from females was slightly higher than males at: 58% females versus 42% males as shown in Figure 18. A similar distribution of gender frequencies has been in a number of studies on e-learning and therefore, is a representative of the population of e-learners (Chua & Montalbo, 2014; One & Lai, 2006; Suri & Sharma, 2013).
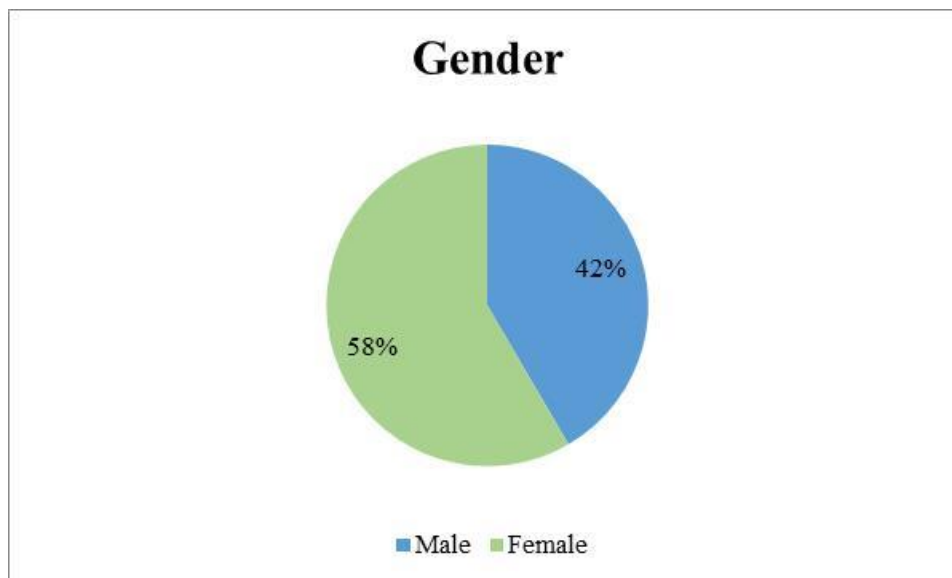
Figure 18. Demographic Distribution for Gender (N=1,070)

The age of most of the respondents were between 20 and 49 accounting for approximately 90% of the sample. The population mean for e-learners is an average of 34, therefore, the sample mean age was also a representation of the population (One & Lai, 2006). Figure 19 depicts the demographic distribution of age of e-learners within the sample.
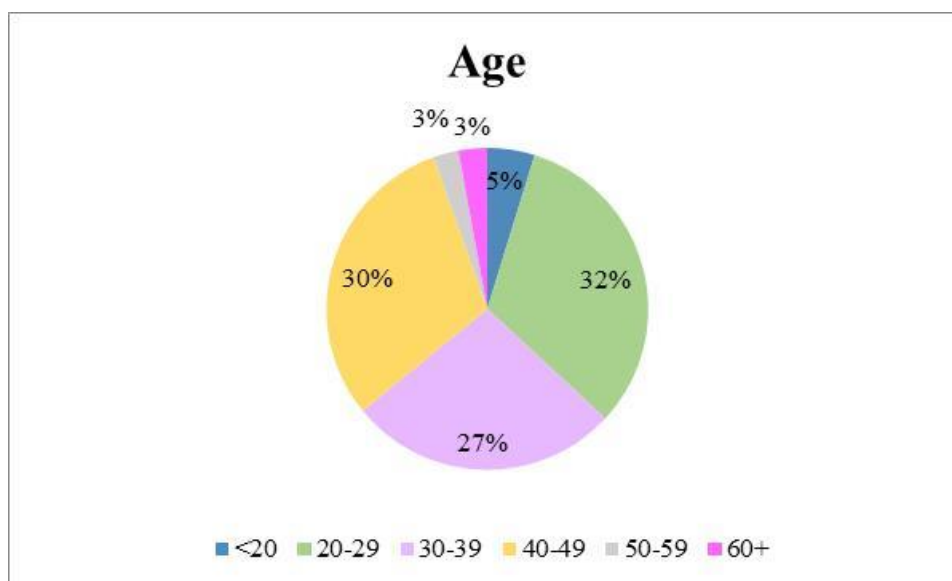
Figure 19. Demographic Distribution for Age (N=1,070)

Finally, over half of the respondents had completed at least six to ten courses in e-learning. The population mean of e-learners was ten completed courses, therefore, the sample mean e-learning experience was also a representation of the population (One & Lai, 2006). Figure 20 depicts the demographic distribution of e-learning experience within the sample.
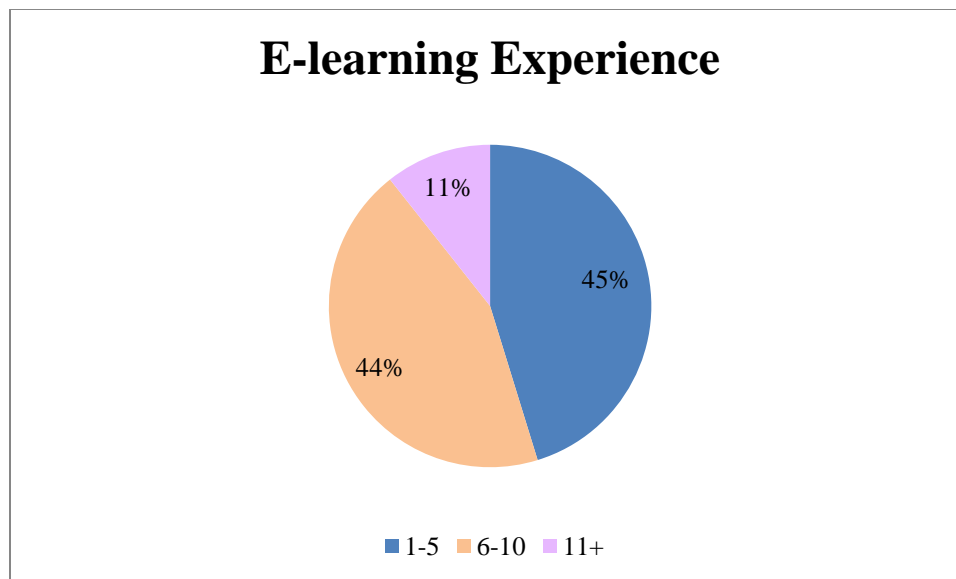
Figure 20. Demographic Distribution for E-learning Experience (N=1,070)

Demographic responses were analyzed against the perception of high potential for threats of impersonation resulting from the paired sample t-test completed on the means for UP-HPI and PP-HPI using an analysis of covariance (ANCOVA). In the ANCOVA, gender was treated as the control variable, which was measured against the mean responses for the 18 e-learning activities to see if there were significant differences between males and females. In both UP-HPI and PP-HPI only two items showed a significantly difference in means; item 8 and item 17. All other items showed no significant differences. The results are shown Table 22 and Figure 21 as well as Table 23 and Figure 22 respectively.

Table 22. ANCOVA for Gender on UP-HPI (N=1,070)

Item	Male		Female		ANCOVA		*
	Mean	SD	Mean	SD	F	Sig.	
UA1	5.11	1.213	5.02	1.309	1.195	.275	
UA2	3.13	1.138	3.17	1.213	.212	.645	
UA3	3.24	1.118	3.23	1.176	.012	.913	
UA4	5.25	1.364	5.25	1.341	.004	.950	
UA5	5.20	1.390	5.20	1.341	.000	.997	
UA6	3.38	1.099	3.46	1.176	1.505	.220	
UA7	3.38	1.121	3.46	1.186	1.468	.226	
UA8	3.18	1.258	3.34	1.297	4.175	**.041**	*
UA9	3.36	1.194	3.47	1.225	2.149	.143	
UA10	5.44	1.556	5.30	1.650	1.785	.182	
UA11	5.43	1.546	5.29	1.650	1.829	.177	
UA12	5.21	1.591	5.07	1.715	1.930	.165	
UA13	5.21	1.600	5.07	1.712	1.774	.183	
UA14	2.39	.885	2.33	.923	1.012	.315	
UA15	2.36	.908	2.33	.940	.221	.638	
UA16	2.35	.917	2.32	.971	.206	.650	
UA17	5.89	1.086	6.05	1.003	6.402	**.012**	*
UA18	2.45	.751	2.36	.859	2.797	.095	

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$
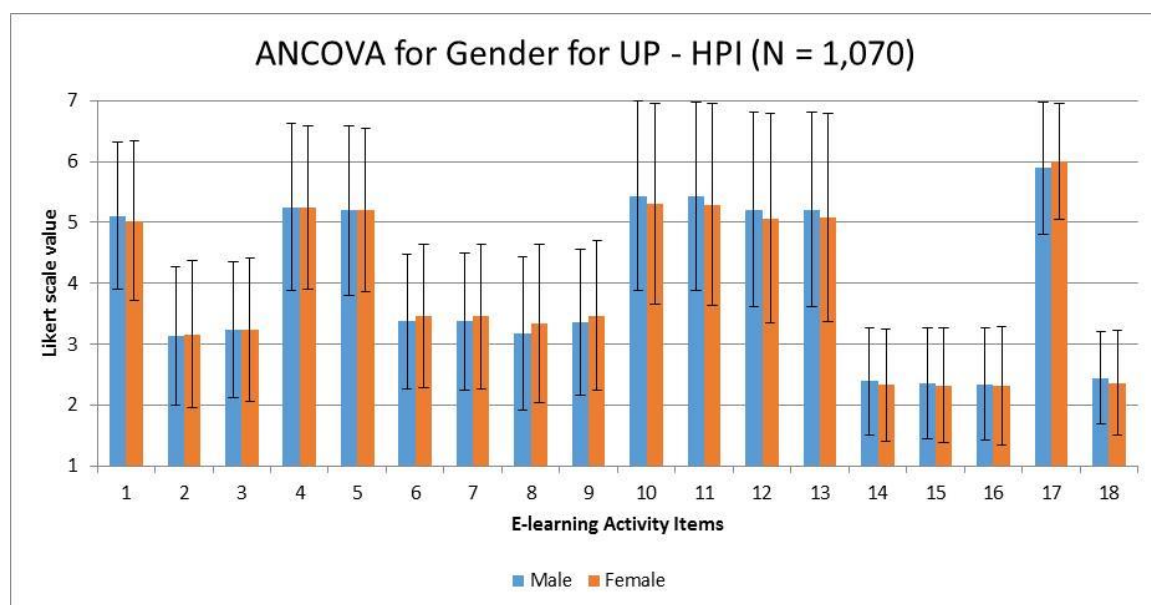
Figure 21. ANCOVA for Gender on UP-HPI (N=1,070)

Table 23. ANCOVA for Gender on PP-HPI (N=1,070)

	Male		Female		ANCOVA		*
Item	Mean	SD	Mean	SD	F	Sig.	
PA1	5.07	1.348	5.05	1.410	1.195	.275	
PA2	2.95	1.213	2.97	1.281	.212	.645	
PA3	3.18	1.129	3.19	1.206	.012	.913	
PA4	5.20	1.434	5.21	1.380	.004	.950	
PA5	5.16	1.417	5.17	1.348	.000	.997	
PA6	3.19	1.253	3.18	1.321	1.505	.220	
PA7	3.38	1.151	3.45	1.206	1.468	.226	
PA8	2.97	1.327	3.04	1.368	4.175	**.041**	*
PA9	3.34	1.209	3.46	1.231	2.149	.143	
PA10	5.37	1.589	5.24	1.668	1.785	.182	
PA11	5.42	1.563	5.27	1.665	1.829	.177	
PA12	5.19	1.604	5.04	1.715	1.930	.165	
PA13	5.19	1.596	5.04	1.710	1.774	.183	
PA14	2.37	.896	2.30	.912	1.012	.315	
PA15	2.34	.906	2.31	.937	.221	.638	
PA16	2.34	.911	2.32	.936	.206	.650	
PA17	5.78	1.052	5.92	.957	6.402	**.012**	*
PA18	2.45	.757	2.36	.867	2.797	.095	

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$
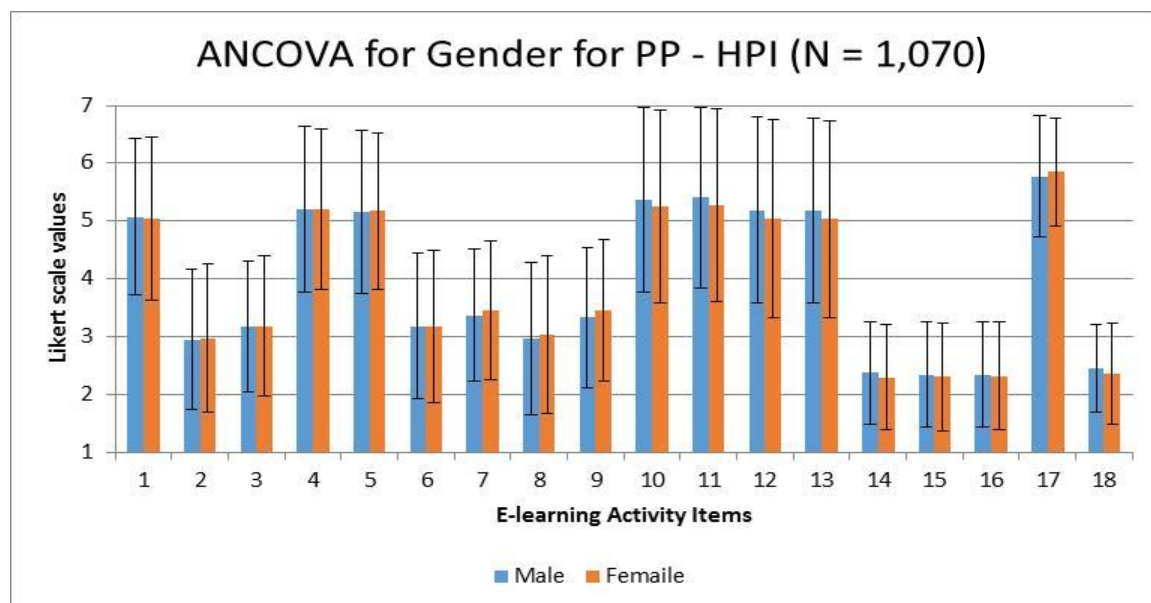
Figure 22. ANCOVA for Gender on PP-HPI (N=1,070)

In the second set of ANCOVA analysis, age was treated as the control variable, which was measured against the mean responses for the 18 e-learning activities to see if there were significant differences between age groups. In only UP-HPI, item 9 showed a significantly difference in means. All other items showed no significant differences. The results are shown Table 24 and Figure 23 as well as Table 25 and Figure 24.

Table 24. ANCOVA for Age on UP-HPI (N=1,070)

Item	<20 Mean	SD	20-29 Mean	SD	30-39 Mean	SD	40-49 Mean	SD	50-59 Mean	SD	60+ Mean	SD	ANCOVA f	sig	*
UA1	5.16	1.173	5.02	1.244	5.10	1.296	5.06	1.290	4.93	1.385	5.10	1.221	.238	.946	
UA2	3.02	1.175	3.23	1.203	3.13	1.168	3.14	1.172	2.89	.934	3.03	1.402	.749	.587	
UA3	3.12	1.336	3.31	1.170	3.21	1.096	3.20	1.162	3.11	.847	3.23	1.283	.548	.740	
UA4	5.25	1.495	5.26	1.322	5.35	1.329	5.10	1.395	5.33	1.414	5.65	.915	1.640	.146	
UA5	5.10	1.565	5.22	1.340	5.27	1.348	5.08	1.391	5.30	1.295	5.55	1.028	1.126	.345	
UA6	3.43	1.188	3.51	1.145	3.37	1.145	3.42	1.134	3.22	.934	3.23	1.359	.853	.512	
UA7	3.39	1.168	3.49	1.158	3.38	1.193	3.44	1.151	3.19	.681	3.29	1.296	.623	.682	
UA8	3.31	1.273	3.35	1.309	3.24	1.247	3.27	1.297	2.85	.818	3.00	1.483	1.141	.337	
UA9	3.37	1.264	3.55	1.202	3.33	1.172	3.46	1.232	2.96	.940	3.10	1.469	2.350	**.039**	*
UA10	5.41	1.590	5.38	1.622	5.37	1.650	5.35	1.561	4.96	1.629	5.39	1.764	.354	.880	
UA11	5.29	1.579	5.40	1.618	5.36	1.641	5.34	1.564	4.96	1.629	5.35	1.743	.384	.860	
UA12	5.14	1.575	5.18	1.677	5.15	1.673	5.08	1.634	4.70	1.793	5.10	1.868	.481	.790	
UA13	5.06	1.567	5.16	1.670	5.16	1.694	5.09	1.625	4.81	1.841	5.29	1.883	.360	.876	
UA14	2.20	.849	2.43	.939	2.33	.826	2.35	.929	2.37	.742	2.19	1.223	1.004	.414	
UA15	2.24	.815	2.39	.968	2.32	.849	2.35	.944	2.30	.775	2.16	1.241	.588	.709	
UA16	2.27	.896	2.38	1.001	2.30	.869	2.33	.952	2.33	.734	2.16	1.267	.513	.767	
UA17	5.96	1.199	6.05	.989	5.96	1.018	5.94	1.071	5.81	1.302	6.26	.965	.994	.420	
UA18	2.39	.896	2.40	.826	2.43	.812	2.40	.805	2.33	.784	2.23	.805	.397	.851	

*** p < 0.001, ** p < 0.01, * p < 0.05
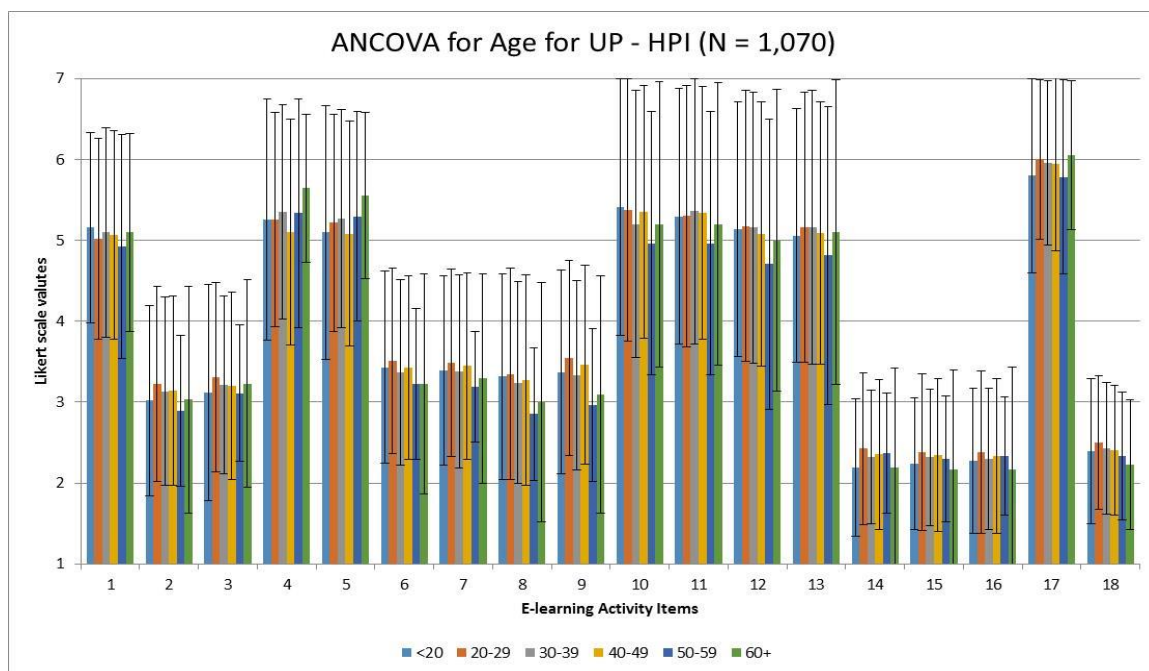
Figure 23. ANCOVA for Age on UP-HPI (N=1,070)

Table 25. ANCOVA for Age on PP-HPI (N=1,070)

Item	<20 Mean	SD	20-29 Mean	SD	30-39 Mean	SD	40-49 Mean	SD	50-59 Mean	SD	60+ Mean	SD	ANCOVA f	sig	*
PA1	5.10	1.253	5.03	1.376	5.06	1.401	5.10	1.400	4.85	1.512	5.00	1.317	.213	.957	
PA2	2.94	1.190	3.03	1.276	2.98	1.216	2.91	1.272	2.74	1.059	2.81	1.424	.557	.733	
PA3	3.31	1.378	3.21	1.247	3.14	1.084	3.19	1.147	2.93	.917	3.29	1.296	.567	.725	
PA4	5.24	1.544	5.23	1.362	5.29	1.406	5.06	1.440	5.26	1.430	5.58	1.057	1.322	.252	
PA5	5.08	1.598	5.19	1.339	5.23	1.354	5.05	1.429	5.30	1.295	5.55	1.028	1.166	.324	
PA6	3.02	1.319	3.26	1.316	3.14	1.264	3.20	1.293	2.93	1.141	3.00	1.390	.804	.547	
PA7	3.37	1.148	3.48	1.175	3.38	1.208	3.44	1.198	3.19	.736	3.29	1.296	.523	.759	
PA8	2.82	1.452	3.00	1.404	2.98	1.320	3.06	1.315	2.81	1.210	3.26	1.390	.648	.663	
PA9	3.35	1.262	3.51	1.224	3.34	1.182	3.44	1.238	2.93	.917	3.10	1.469	2.049	.069	
PA10	5.39	1.601	5.33	1.678	5.30	1.658	5.29	1.567	4.81	1.711	5.29	1.716	.531	.753	
PA11	5.27	1.626	5.39	1.623	5.33	1.640	5.32	1.587	4.85	1.812	5.39	1.745	.573	.721	
PA12	5.14	1.600	5.15	1.689	5.13	1.657	5.06	1.656	4.70	1.706	5.03	1.906	.413	.840	
PA13	5.06	1.555	5.14	1.672	5.12	1.676	5.06	1.634	4.70	1.836	5.29	1.883	.469	.799	
PA14	2.16	.857	2.40	.920	2.30	.849	2.33	0.921	2.33	.784	2.19	1.223	.942	.453	
PA15	2.22	.832	2.38	.962	2.30	.857	2.33	0.931	2.22	.847	2.13	1.204	.785	.560	
PA16	2.25	.821	2.37	.966	2.30	.850	2.35	0.942	2.26	.764	2.23	1.257	.379	.863	
PA17	5.84	1.223	5.93	.945	5.84	.973	5.80	1.016	5.67	1.330	6.10	.908	1.119	.348	
PA18	2.39	.896	2.40	.837	2.43	.820	2.40	0.808	2.33	.784	2.23	.805	.374	.867	

*** p < 0.001, ** p < 0.01, * p < 0.05
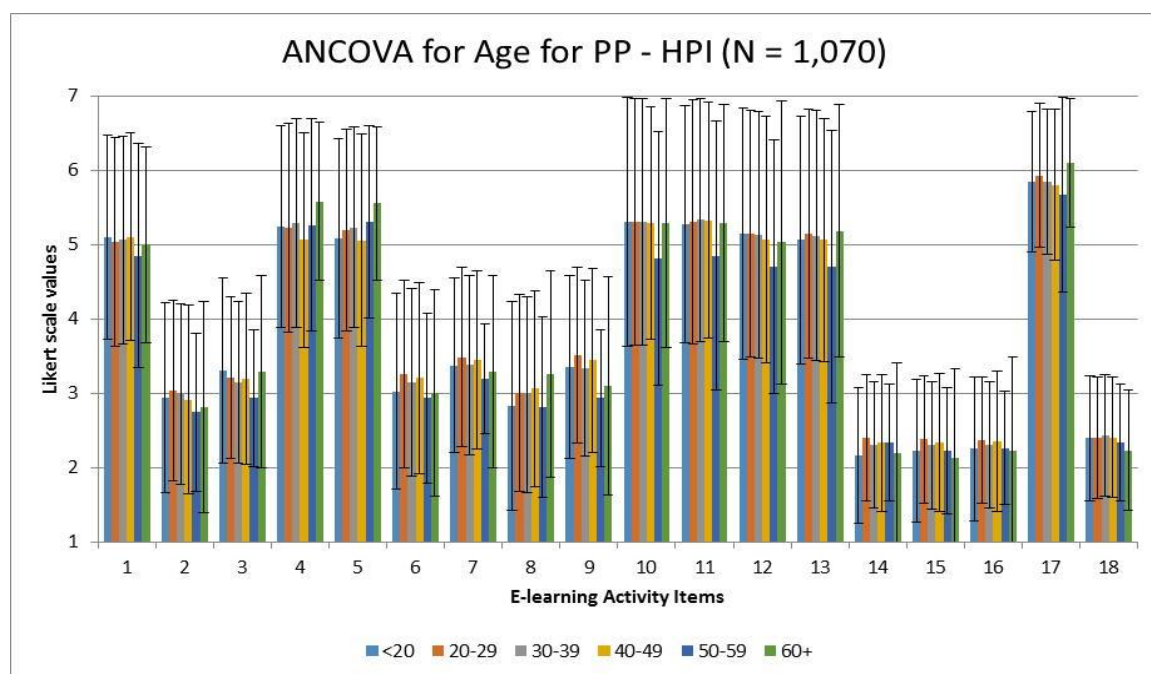
Figure 24. ANCOVA for Age on PP-HPI (N=1,070)

In the third set of ANCOVA analysis, e-learning experience was treated as the control variable, which was measured against the mean responses for the 18 e-learning activities to see if there were significant differences between e-learning experience groups. In both UP-HPI and PP-HPI no items showed any significant differences. The results are shown Table 26 and Figure 24 as well as Table 27 and Figure 25.

Table 26. ANCOVA for E-learning Experience on UP-HPI (in # of courses) (N=1,070)

Item	1-5		6-10		11+		ANCOVA		*
	Mean	SD	Mean	SD	Mean	SD	f	sig	
UA1	5.07	1.257	5.06	1.277	5.02	1.303	.079	.924	
UA2	3.12	1.166	3.19	1.202	3.11	1.173	.447	.640	
UA3	3.18	1.151	3.29	1.164	3.22	1.103	1.153	.316	
UA4	5.23	1.358	5.26	1.353	5.31	1.311	.175	.840	
UA5	5.19	1.366	5.20	1.378	5.20	1.277	.003	.997	
UA6	3.40	1.115	3.46	1.180	3.39	1.134	.410	.663	
UA7	3.40	1.135	3.46	1.174	3.40	1.210	.354	.702	
UA8	3.25	1.255	3.29	1.316	3.25	1.268	.127	.880	
UA9	3.40	1.201	3.44	1.221	3.47	1.235	.227	.797	
UA10	5.39	1.621	5.36	1.580	5.22	1.708	.533	.587	
UA11	5.38	1.618	5.33	1.587	5.29	1.660	.225	.798	
UA12	5.16	1.676	5.10	1.648	5.11	1.700	.162	.851	
UA13	5.16	1.672	5.11	1.650	5.07	1.723	.196	.822	
UA14	2.33	.927	2.40	.905	2.29	.828	1.206	.300	
UA15	2.33	.951	2.36	.918	2.28	.857	.434	.648	
UA16	2.31	.988	2.36	.928	2.29	.859	.497	.608	
UA17	5.94	1.078	5.99	1.032	6.15	.895	1.793	.167	
UA18	2.41	.841	2.40	.813	2.33	.725	.445	.641	

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$
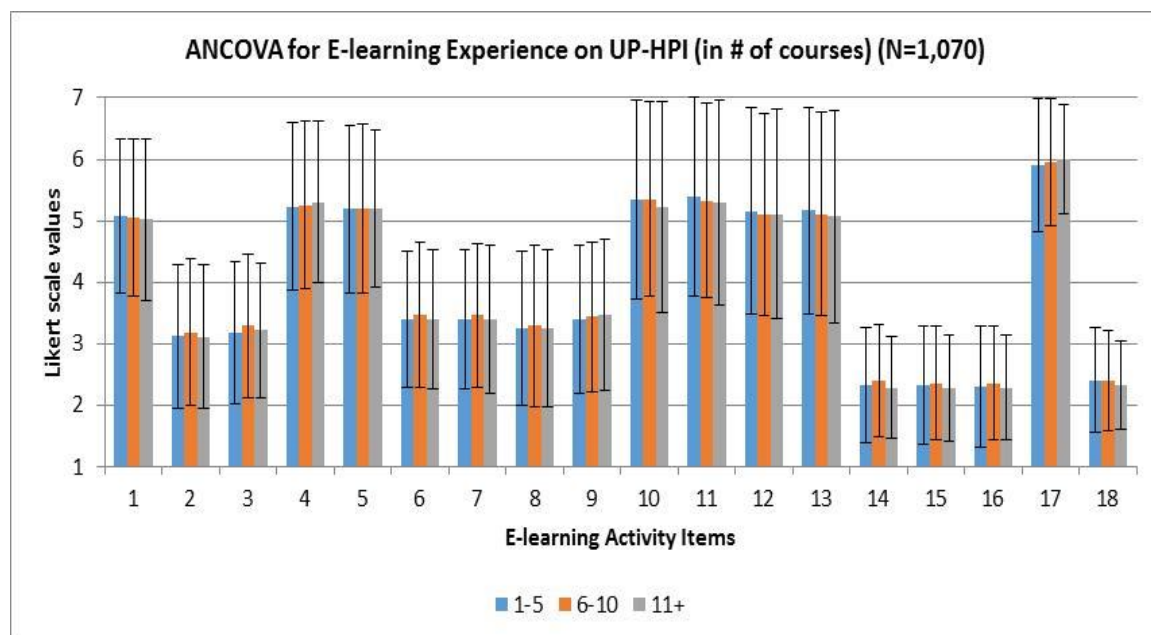
Figure 25. ANCOVA for E-learning Experience on UP-HPI (N=1,070)

Table 27. ANCOVA for E-learning Experience on PP-HPI (in # of courses) (N=1,070)

Item	1-5		6-10		11+		ANCOVA		
	Mean	SD	Mean	SD	Mean	SD	f	sig	*
PA1	5.07	1.363	5.05	1.403	5.04	1.404	.079	.924	
PA2	2.92	1.239	3.00	1.274	2.99	1.230	.447	.640	
PA3	3.15	1.170	3.23	1.194	3.13	1.109	1.153	.316	
PA4	5.20	1.393	5.20	1.427	5.25	1.349	.175	.840	
PA5	5.18	1.364	5.15	1.408	5.18	1.307	.003	.997	
PA6	3.21	1.291	3.15	1.306	3.16	1.252	.410	.663	
PA7	3.41	1.168	3.43	1.198	3.43	1.197	.354	.702	
PA8	3.01	1.352	3.03	1.356	2.96	1.333	.127	.880	
PA9	3.37	1.204	3.44	1.242	3.49	1.228	.227	.797	
PA10	5.34	1.646	5.30	1.604	5.11	1.726	.533	.587	
PA11	5.36	1.633	5.31	1.604	5.28	1.680	.225	.798	
PA12	5.12	1.682	5.08	1.651	5.07	1.718	.162	.851	
PA13	5.12	1.670	5.10	1.645	5.04	1.734	.196	.822	
PA14	2.30	.931	2.37	.900	2.27	.812	1.206	.300	
PA15	2.31	.952	2.35	.911	2.28	.857	.434	.648	
PA16	2.32	.949	2.36	.918	2.26	.852	.497	.608	
PA17	5.81	1.045	5.87	.982	6.03	.846	1.793	.167	
PA18	2.42	.846	2.39	.823	2.35	.728	.445	.641	

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$
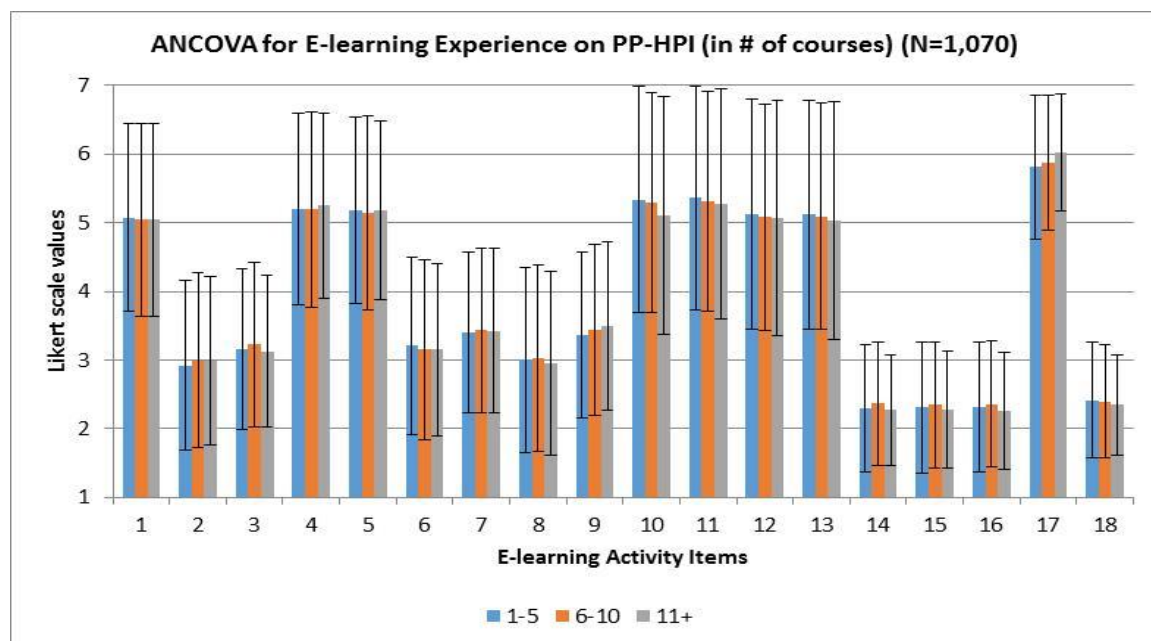
Figure 26. ANCOVA for E-learning Experience on PP-HPI (N=1,070)

The fourth goal of this study was to determine if there were significant differences among the demographic variable and perception of high potential for threats of impersonation. As seen in the results, only a few items showed a significant difference; item 8 and 17 for both UP-HPI and PP-HPI for females. And item 9 for UP-HPI in the 20-29 age group. Overall a large majority showed no significant differences on any of the demographic variable for the items assessed.

Summary

In this chapter, a thorough analysis was conducted using the data collected from participants via a validated Web-based survey in order to answer the twelve research questions in this study. The methodology consisted of three phases for this study. Phase one was an exploratory study conducted through a literature review in order to develop a new survey instrument adapted from previous studies. Phase two used the Delphi method to acquire an expert panel to gather feedback for revisions to the survey in order to ensure instrument validity. The results of phase two were presented in a table, which described the specific feedback and revisions necessary to produce a final survey instrument to collect the data for this study. The final revised survey instrument designed using Qualtrics is found in Appendix A of this study. Phase three involved gathering the data for an extensive quantitative analysis. A participation letter and link to the Web-based survey was sent to over 15,000 e-learners. A total of 1,086 responses were collected equally a response rate of 7.2%. After the pre-analysis screening of the data to remove response-set responses and outliers, the sample included 1,070 participants who had

completed at least one online course. A summary of the findings from the quantitative

analysis for the research questions are summarized below in Table 28:

Table 28. A Summary of Research Questions and the Findings

Research Questions	Data Analysis	Findings
RQ1a: What e-learning activities are perceived by users to have a high potential for threats of impersonation?	Used descriptive statistics to calculate means and SDs from lowest to highest.	22% of items have a high potential for threats of impersonation.
RQ1b: What e-learning activities users perceived that their peers will identify to have a high potential for threats of impersonation?	Used descriptive statistics to calculate means and SDs from lowest to highest.	28% of items have a high potential for threats of impersonation.
RQ1c: How do the e-learning activities perceived by users to have a high potential for impersonation differ than what is perceived by users that their peers will identify?	Compared means using a paired sample t-test.	12 out of 18 e-learning activities had a significant difference in perception of high potential for impersonation between the groups.
RQ2a: What levels of authentication strength are perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities?	Used descriptive statistics to calculate means and SDs from highest to lowest.	Identified the following suitable level for e-learning activities: 11% Strong Authentication (live-proctor) 17% Moderate – Low (biometric) 72% Very low (Password)

Table 28. A Summary of Research Questions and the Findings (continued)

Research Questions	Data Analysis	Findings
RQ2b: What levels of authentication strength are perceived by users that their peers will identify to be most suitable against the threats of impersonation for these assessed e-learning activities?	Used descriptive statistics to calculate means and SDs from highest to lowest.	Identified the following suitable level for e-learning activities: 11% Strong Authentication (live-proctor) 17% Moderate – Low (biometric) 72% Very low (Password)
RQ2c: How do the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities differ than what is perceived by users that their peers will identify?	Compared means using a paired sample t-test	9 out of 18 e-learning activities had a significant difference in levels of authentication strength for e-learning activities between the groups.
RQ3a: What are the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities?	EFA using PCA were used to retain significant components using Varimax rotation. Cronbach's Alpha reliability test was run on retain components.	8 significant components identified via PCA 7 components retained via Cronbach's alpha

Table 28. A Summary of Research Questions and the Findings (continued)

Research Questions	Data Analysis	Findings
RQ3b: What are the significant components of the levels of authentication strength perceived by users that their peers will identify to be most suitable against the threats of impersonation for these assessed e-learning activities?	EFA using PCA were used to retain significant components using Varimax rotation. Cronbach's Alpha reliability test was run on retain components.	8 significant components identified via PCA 7 components retained via Cronbach's Alpha
RQ3c: What are the differences between the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities versus than what is perceived by users that their peers will identify?	Used the literature review to discuss the findings.	The same 7 significant components were identified between RQ3a and RQ3b. Components were categorized and organized into a list of e-learning activities by factor.

The final three research questions RQ4a, RQ4b, and RQ4c were analyzed to identify significant differences in perception of high potential for threats of impersonation based upon gender (RQ4a), age (RQ4b), and e-learning experience (RQ4c). An ANCOVA test was performed to compare the means of the two groups against each control demographic variable. The ANCOVA test indicated that overall there are no significant differences in perception of high potential for threats of impersonation based upon gender, age, and e-learning experience.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Overview

In this chapter, conclusions are drawn and discussed based upon the analysis

performed within this study. The research questions are examined in context of the results

achieved along with any limitations of the study. The implications for study and the

contribution to the body of knowledge within the IS field of study is discussed as well as

recommendations for future research. Finally, a summary concludes this chapter of the

study.

Conclusions

To reiterate, the main goal of this proposed research study was to empirically assess

what *authentication methods* and *strength* users perceived to be most suitable for

activities in e-learning systems based on the threats of impersonation. This study was

built on a previous study by Apampa et al. (2010) that identified impersonation fraud as a

major threat to summative e-assessments and previous studies, which identified critical e-

learning activities used in e-learning systems (Adams, 2012; Bailie & Jortberg, 2009;

Levy, 2006b). A set of 12 research questions were developed for this exploratory

research study to be analyzed and discussed based on the data collected by the Web-

based survey.

The research questions (RQ1a & RQ1b) used to identify what e-learning activities perceived by users and users perceived that their peers will identify to have a high potential for impersonation presented a ranked list of e-learning activities from lowest to highest perceived potential based upon the statistical means for each group. Similarly, descriptive statistics ranked the means from highest to lowest for research questions (RQ2a & RQ2b) that asked what levels of authentication strength are perceived as suitable against the different impersonation fraud by users and users perceived that their peers will identify. The results from both sets of descriptive statistics determined that the same four items that not only have a high potential for threat of impersonation but also were determined to need a strong level of authentication to reduce the threat. Seven components were retained and categorized for both groups (RQ3a & RQ3b). Two items that were not retained were determined to need further investigation as to how they should be labeled as either summative or formative activities, which led to a wide variation in responses in terms of authentication strength suitable to reduce threat of impersonation.

There were a few notable limitations of this study. The first limitation is that it is possible that not all respondents have real experience with each authentication control used in the likert scale to measure suitable level of authentication. This limitation was moderated by providing both a description and image to describe the types of levels for authentication strength commonly used in Web-based system. Another limitation is the varying e-learning experience of the participants. Participants with five or more completed online courses may have more experience completing the e-learning activities than those with less e-learning experience.

Implications

The results of this study contributed notably to the body of knowledge, and has several implications within the field of IS as well as for future research in the domain of authentication and IS security. This study used Activity Theory as a lens to compile a list of 18 e-learning activities used in previous studies that were determined to have CVFs in e-learning systems (Engestrom, 2001; Levy, 2008). The research includes an extensive literature review in order to select the types of authentication controls and their respective strengths in order to mitigate the threat of impersonation for an e-learning activity in Web-based systems by deterring misuse. This exploratory research used the TTF framework to create an authentication scale necessary to identify a suitable level of authentication strength to reduce the threat of impersonation for an e-learning activity in Web-based systems. The scale development was supported through an extensive literature review that suggested using a multi-factor authentication versus single-factor authentication creates a stronger level control and is perceived to reduce the likelihood of IS misuse particularly from impersonation fraud (Apampa et al., 2010). The scale created organized the types of levels of authentication strength ranging from extremely low strength to extremely high strength and was validated by an expert panel.

The results of this research imply a number of implications for research and application. Most relevant is that users do perceive the need for different levels of authentication as suitable based upon the activity being completed, as opposed to a 'one size fits all' systems approach. This is due to the perceived high potential of threat of impersonation on selected summative e-assessments such as exams and quizzes. Although 18 e-learning activities were assessed many were viewed as having a low

potential for impersonation due in part to the formative nature of the activity. Only four were consistently identified within an e-learning system as having a high potential for impersonation. The findings in this study are relevant to e-learning providers in both academic and non-academic environments where the possibility of IS misuse due to deliberate impersonation can undermine the value of the system (Apampa et al., 2011). E-learning providers may find it important to incorporate stronger authentication on summative e-assessments. As the findings suggested to reduce the risk deliberate impersonation, formal collaborative activities should use at minimum a two-factor username/password along with biometric authentication to insure identity and high-stakes summative activities should use live-proctor authentication, which offers remote surveillance to insure the identity of the user completing the activity.

Recommendations

This study was exploratory and provided recommended levels of authentication for selected e-learning activities that had a perceived high potential for impersonation. The results have made the case that e-learning systems need to authenticate e-learning activities and not just at the system level to insure the identity of the remote user. The use of stronger multi-factor authentication that includes biometrics and/or live-proctor authentication will reduce the opportunity for deliberate impersonation.

Because this study was exploratory, further research needs to be completed in order to measure if the perception of threat of impersonation is reduced after users have actually been authenticated via biometric or live-proctor authentication. Within the research community, it would be meaningful to conduct an experimental study with the validated

instrument that was developed in this study. Within an experimental study, users can be asked to complete the e-learning activities using varying levels of authentication strength. Carstairs and Myors (2009) claimed that scores are often inflated on summative e-assessments in an un-proctored environment due to IS misuse. The study could seek to determine if the threat of impersonation is reduced based on the use of a stronger authentication for those activities identified to have the highest risk. Users that have had experience with multi-factor authentication may respond differently due to actual hands-on experience. Additionally, two items (submitting assignments & projects) that ranked high in terms of potential for impersonation were not retained within the PCA because of the low factor loads. It is believed, due to the vague, inconsistent categorization of these items (formative &/or summative); it would be valuable for another study to be conducted with those items being specifically categorized as summative in order to improve loads and properly categorize them. Finally, this study sought to determine responses from e-learning users only. Another future study could complete a similar study with facilitators of e-learning systems. The responses of the facilitators can be compared with those of this study to further identify suitable levels of authentication for the selected activities with high risk of impersonation. This can explore the relationship between what users versus facilitator perceive as suitable, in order to produce further insight into the effect level of authentication of e-learning activities against the threat of impersonation.

Finally, additional research is required to determine if the use of suitable authentication level significantly reduces the threat of impersonation. What levels are suitable in order to measure a statistically significantly reduction in the threat of

impersonation? Do users and facilitators identify different levels of authentication as suitable in order to reduce impersonation? Does the identified suitable level change once a user has experience with authentication control? Finally, to generalize the findings in this study, future research may develop a similar list of e-learning activities for a non-academic system in order to conduct the same analysis.

Summary

This dissertation study addressed the research problem that a 'one size fits all' authentication method does not secure Web-based systems at the activity level from the risk of deliberate impersonation (Helkala & Snekkenes, 2009). Previous studies have indicated that finding suitable authentication is a significant and challenging problem (Apampa et al., 2010; Bedford et al., 2009; Jalel & Zeb, 2008; Levy and Ramim, 2010). In response, this research explored the need to identify a suitable authentication level specific to an e-learning activity in order to deter IS misuse. This study is unique because it examined 18 e-learning activities that included both summative and formative e-assessments, whereas, previous studies only focused on high-stakes assessments (Penteado & Marana, 2009; Rodchua et al., 2001). Additionally, these studies do not address multi-factor authentication and focus primarily on the use of a single-factor authentication such face recognition or fingerprint technology, which may not be suitable for all types of activities (Helkala & Snekkenes, 2009).

The main goal of this research was to conduct an exploratory study to empirically assess what authentication methods and strength uses perceived to be most suitable for activities in e-learning systems specifically against the threat of impersonation. Furthermore, this study sought to determine if there were significant differences in

response of groups of what users perceived and what users perceived that their peers would identify. Twelve research questions were created in order to explore the research problem. To meet the goals of this study and answer the research questions, a survey instrument along with authentication strength scale based upon an extensive literature review was developed. A Delphi Expert Panel was assembled to solicit feedback to validate the instrument. Once the instrument was approved and no further changes were recommended, sample data was collected from a population of e-learners in order to conduct the data analysis. After pre-screening of the data was completed, 1,070 useful cases were used in an extensive statistical analysis. Based on descriptive statistics, it was determined that there were a specific set of e-learning activities perceived by users and that users perceived that their peers would identify as having a high potential for impersonation. Additionally, the same set of items were identified as needing moderate to high levels of authentication strength in order to reduce the threat of impersonation. A paired sample t-test for means showed that overall there was no significant difference in how the users responded in each group of questions. Significant components were identified and factors were categorized in order to provide a clear list of e-learning activities that are similar in terms of assessment types. Finally, demographic variables were tested for significant differences in responses among gender, age, and e-learning experience. Very few item responses had significant differences in responses.

Impersonation is a major threat in e-learning systems due to wide use of a single-factor authentication such as a username/password as the only means of authenticating a remote user. Often this authentication is done at a single sign-in upon entry of the system. Passwords have very low authentication strength and can easily be given out allowing

someone to deliberately impersonation a user. It has been emphasized that the use of

suitable authentication is imperative in e-learning systems in order to ensure IS security.

The findings of this study indicate that e-learning providers should be aware that the

absence of strong authentication leaves the system vulnerable for impersonation. This

study also suggests that users have identified the need for strong levels of authentication

for summative e-assessments as a means to reduce that threat of impersonation.

1

Appendix A

Survey

Authenticating E-learning Activities Survey

Instructions: Complete the following survey by selecting the most appropriate response for each question. The information gathered will be used for research to understand what e-learning activities are at risk of impersonation and what authentication strength is suitable to protect against impersonation. All responses are anonymous and cannot be linked to you in anyway. Completion of this Web-based survey indicates your voluntary participation in the study.

Section A

Using the follow definitions please select the best response:

E-learning activities - an educational procedure designed to stimulate learning by online experience utilizing online learning systems and tools.

Impersonation - a fraudulent action with the aim of imitating a legitimate user and defrauding the security system.

Select a response for both the User (U) and Peer (P) group for the 18 E-learning Activities listed below:

	(U) I think this e-learning activity has a high potential for impersonation fraud by users.							(P) I think my peers will identify that this e-learning activity has a high potential for impersonation fraud by users.						
	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree
1. Develop a personal Website, profile, or blog	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍
2. Participate in text-chat sessions with the professor	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍
3. Participate in text-chat sessions with other students	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍

	(U) I think this e-learning activity has a high potential for impersonation fraud by users.							(P) I think my peers will identify that this e-learning activity has a high potential for impersonation fraud by users.						
	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree
4. Participate in live voice-chat sessions with the professor	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5. Participate in live voice-chat sessions with other students	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6. .Post in new discussion forum message to the professor	○	○	○	○	○	○	○	○	○	○	○	○	○	○

	(U) I think this e-learning activity has a high potential for impersonation fraud by users.							(P) I think my peers will identify that this e-learning activity has a high potential for impersonation fraud by users.						
	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree
7. Post in new discussion forum message with other students	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8. Reply to discussion forum messages to the professor	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9. Reply to discussion forum messages with other students	○	○	○	○	○	○	○	○	○	○	○	○	○	○

	(U) I think this e-learning activity has a high potential for impersonation fraud by users.							(P) I think my peers will identify that this e-learning activity has a high potential for impersonation fraud by users.						
	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree
10. Send e-mails to other students	○	○	○	○	○	○	○	○	○	○	○	○	○	○
11. Send e-mails to the professor	○	○	○	○	○	○	○	○	○	○	○	○	○	○
12. Share assignments with other students (via discussion forum)	○	○	○	○	○	○	○	○	○	○	○	○	○	○

	(U) I think this e-learning activity has a high potential for impersonation fraud by users.							(P) I think my peers will identify that this e-learning activity has a high potential for impersonation fraud by users.						
	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree
13. Share assignments with other students (via e-mail)	○	○	○	○	○	○	○	○	○	○	○	○	○	○
14. Submit assignments online	○	○	○	○	○	○	○	○	○	○	○	○	○	○
15. Submit exams online	○	○	○	○	○	○	○	○	○	○	○	○	○	○

	(U) I think this e-learning activity has a high potential for impersonation fraud by users.							(P) I think my peers will identify that this e-learning activity has a high potential for impersonation fraud by users.						
	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree	(1) Strongly Agree	(2) Agree	(3) Somewhat Agree	(4) Neither Agree or Disagree	(5) Somewhat Disagree	(6) Disagree	(7) Strongly Disagree
16. Submit quizzes online	○	○	○	○	○	○	○	○	○	○	○	○	○	○
17. Submit ungraded practice quizzes online	○	○	○	○	○	○	○	○	○	○	○	○	○	○
18. Submit projects online	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Section B

Using the follow definitions please select the best response:

Authentication - the process of verifying an attempted request of an individual (i.e. "the user") to gain access to a system.

Token - stored information about one or more authentication methods: i.e. an ATM or ID Card with magnetic stripe

Biometrics - the identification of an individual based on physiological and behavioral characteristics.

Live-proctor - observation of remote e-learners via a Web-cam and a live proctor over the internet

Types of levels for authentication strength:

Username/Password, Token, Biometric Finger Scanning, and Live-Proctoring equipment are depicted below:

Select a response for both the User (U) and Peer (P) group for the 18 E-learning Activities listed below:

	(U) I think the selected Authentication Strength is suitable for the e-learning activity to reduce impersonation fraud.							(P) I think my peers will identify the selected Authentication Strength as suitable for the e-learning activity to reduce impersonation fraud.						
	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)
1. Develop a personal Website, profile, or blog	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2. Participate in text-chat sessions with the professor	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3. Participate in text-chat sessions with other students	○	○	○	○	○	○	○	○	○	○	○	○	○	○

	(U) I think the selected Authentication Strength is suitable for the e-learning activity to reduce impersonation fraud.							(P) I think my peers will identify the selected Authentication Strength as suitable for the e-learning activity to reduce impersonation fraud.						
	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)
4. Participate in live voice-chat sessions with professor	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5. Participate in live voice-chat sessions with other students	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6. Post in new discussion forum message to the professor	○	○	○	○	○	○	○	○	○	○	○	○	○	○

	(U) I think the selected Authentication Strength is suitable for the e-learning activity to reduce impersonation fraud.							(P) I think my peers will identify the selected Authentication Strength as suitable for the e-learning activity to reduce impersonation fraud.						
	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)
7. Post in new discussion forum message to other students	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8. Reply to discussion forum messages to the professor	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9. Reply to discussion forum messages to other students	○	○	○	○	○	○	○	○	○	○	○	○	○	○

	(U) I think the selected Authentication Strength is suitable for the e-learning activity to reduce impersonation fraud.							(P) I think my peers will identify the selected Authentication Strength as suitable for the e-learning activity to reduce impersonation fraud.						
	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)
10. Send e-mails to other students	○	○	○	○	○	○	○	○	○	○	○	○	○	○
11. Send e-mails to the professor	○	○	○	○	○	○	○	○	○	○	○	○	○	○
12. Share assignments with other students (via discussion forum)	○	○	○	○	○	○	○	○	○	○	○	○	○	○

	(U) I think the selected Authentication Strength is suitable for the e-learning activity to reduce impersonation fraud.							(P) I think my peers will identify the selected Authentication Strength as suitable for the e-learning activity to reduce impersonation fraud.						
	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)
13. Share assignments with other students (via e-mail)	○	○	○	○	○	○	○	○	○	○	○	○	○	○
14. Submit assignments online	○	○	○	○	○	○	○	○	○	○	○	○	○	○
15. Submit exams online	○	○	○	○	○	○	○	○	○	○	○	○	○	○

	(U) I think the selected Authentication Strength is suitable for the e-learning activity to reduce impersonation fraud.							(P) I think my peers will identify the selected Authentication Strength as suitable for the e-learning activity to reduce impersonation fraud.						
	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)	(1) Extremely Low Strength (Password)	(2) Very Low Strength (Token)	(3) Low Strength (Biometric)	(4) Moderate Strength (Password & Biometric)	(5) High Strength (Password & Live-Proctor)	(6) Very High Strength (Biometric & Live-Proctor)	(7) Extremely High Strength (Password, Biometric, & Live-Proctor)
16. Submit quizzes online	○	○	○	○	○	○	○	○	○	○	○	○	○	○
17. Submit ungraded practice quizzes online	○	○	○	○	○	○	○	○	○	○	○	○	○	○
18. Submit projects online	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Section C: Demographic Information

DEM1 What is your gender?

○ Male
○ Female

DEM2 What is your age?

○ Under 20
○ 20 - 29
○ 30 - 39
○ 40 - 49
○ 50 - 59
○ 60 or Over

DEM3 How many online classes have you completed?

○ None
○ 1-5
○ 6-10
○ 11+

Appendix B

Participation Letter

Subject: Authenticating E-learning Activities Web-based Survey

Dear [student name],

I am writing to request your help with an important research study I am conducting to complete my doctoral dissertation at Nova Southeastern University. You are invited to participate in a Web-based survey regarding authenticating e-learning activities used as assessments in e-learning systems. You were selected to be part of this study because you are a student who has participated in e-learning at a University.

I know that this is a busy time of year for you, but I hope that you will take just a little time to participate in the brief survey I will send to you in one week. The information gathered will be used for research to understand what e-learning activities are at risk of impersonation and what authentication strength is suitable to protect them against impersonation.

To make participation as convenient as possible, you will be receiving a link to the Web-based survey to complete at your leisure. The survey itself should take no more than 30 minutes to complete. All responses are anonymous and cannot be linked to you in anyway.

Thank you in advance for your participation in this important study. If you have any questions about the administration of the survey, please contact me at sb1324@nova.edu.

Sincerely,

Shauna Beaudin, Ph.D. Candidate
Nova Southeastern University

Appendix C

Approval Letter to Collect Data

Proctor U

July 17, 2014

TO WHOM IT MAY CONCERN:

Shauna Beaudin is conducting a dissertation study regarding suitable authentication for specific e-learning activities. Mrs. Beaudin has demonstrated ample experience in the field of e-learning. As IT Director, Mrs. Beaudin was responsible for implementing industry training and certification through a variety of Web-based systems. Additionally, Mrs. Beaudin has served as a faculty member teaching numerous e-learning courses at universities in the Northeast and is currently employed as a lecturer in Information Technology at Southern New Hampshire University.

This is a confirmation that Mrs. Shauna Beaudin has been approved to collect research data for her study entitled "An Empirical Study of Authentication Methods to Secure E-learning System Activities Against Impersonation Fraud". Shauna Beaudin has permission to administer a Web-based survey to users of participating institutions that are affiliated with ProctorU who are relevant to the study. The results of the study will contribute to the body of knowledge in the field of Information Systems. Additionally, the benefits will be significant to ProctorU as it relates to the practices of authenticating users of e-learning systems.

We look forward to supporting Mrs. Beaudin in her research and eagerly anticipate the findings.

Sincerely,

Jarrod H. Morgan
Executive Vice President

Appendix D

IRB Approval Letter

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

NSU

MEMORANDUM

To: Shauna Beaudin

From: Ling Wang, Ph.D.
          Institutional Review Board

Date: July 30, 2014

Re: *An Empirical Study of Authentication Methods to Secure E-learning System Activities Against Impersonation Fraud*

IRB Approval Number: wang07151402

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1)   CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2)   ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3)   AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

References

Aceves, P. A., & Aceves, R. I. (2009). Student identity and authentication in distance education: A primer for distance learning administrators. *Continuing Higher Education Review, 73*, 143-152.

Adams, F. (2012). Who's who in distance education: Authentication and academic integrity. *Distance Learning, 9*(1), 13-19.

Al-Assam, H., Sellahewa, H., & Jassim, S. (2011). Accuracy and security evaluation of multi-factor biometric authentication. *International Journal for Information Security Research, 1/2*(1), 11-19.

Al-Khouri, A. M., & Bal, J. (2007). Digital identities and the promise of the technology trio: PKI, smart cards, and biometrics. *Journal of Computer Science, 3*(6), 361.

Alwi, N., & Fan, I. (2010). E-learning and information system management. *International Journal of Digital Society, 1*(2), 148-156.

Apampa, K. M., Wills, G. B., Argles, D., & Marais, E. (2008). Electronic integrity issues in e-assessment security. *Proceedings from ICALT 2008: The Eighth IEEE International Conference on Advanced Learning*. Spain.

Apampa, K. M., Wills, G., & Argles, D. (2010). User security issues in summative e-assessment security. *International Journal of Digital Society, 1*(2), 135-147.

Apampa, K. M., Wills, G., & Argles, D. (2011). Towards a blob-based presence verification system in summative e-assessments. *International Journal of e-Assessment, 1*(1).

Asha, C., & Chellappan, C. (2008). Authentication of e-learners using multimodal biometric technology. *Proceedings from ISBAST 2008: International Symposium on Biometrics and Security Technologies,* 1-6.

Bailie, J. L., & Jortberg, M. A. (2009). Online learner authentication: Verifying the identity of online user's. *Journal of Online Learning and Teaching, 5*(2), 197-207.

Bedford, W., Gregg, J., & Clinton, S. (2009). Implementing technology to prevent online cheating: a case study at a small southern regional university (SSRU). *Journal of Online Learning and Teaching, 5*(2), 230-238.

Berge, Z., & Giles, L. (2008). Implementing and sustaining e-learning in the workplace. *International Journal of Web-based Learning and Teaching Technologies, 3*(3), 44-53.

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly, 27*(3), 264-271.

Bhargav-Spantzel, A., Squicciarini, A. C., & Bertino, E. (2007). Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security, 15*(5), 529-560.

Bolle, R., Connell, J., Pankanti, S., Ratha, N., & Senior, A. (2003) *Guide to Biometrics Springer Professional Computing.* New York Inc.: Springer-Verlag.

Bondarouk, T., & Ruël, H. (2010). Dynamics of e-learning: theoretical and practical perspectives. *International Journal of Training and Development, 14*(3), 149-154.

Boudreau, M. C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly, 25*(1), 1-16.

Brent, E., & Atkisson, C. (2011). Accounting for cheating: An evolving theory and emergent themes. *Research in Higher Education, 52*(6), 640-658.

Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., Polk, W. T., Gupta, S., & Nabbus, E. A. (2013). *Electronic Authentication Guideline. NIST Special Publication 800-63-2.*

Calderon, T. G., Chandra, A., & Cheh J. J. (2006). Modeling an intelligent continuous authentication system to protect financial information resources. *International Journal of Accounting Information Systems, 7*(2), 91-109.

Caloyannides, M., Copeland, D. R., Datesman, G. H., & Weitzel, D. S. (2003). US e-government authentication framework and programs. *IT professional, 5*(3), 16-21.

Campbell, D. T., (1957) Factors relevant to the validity of experiments in social settings. *Psychological Bulletin, 54*(4), 297–312.

Cheng, B., Wang, M., Yang, S. J., & Peng, K. (2011) Acceptance of competency-based workplace e-learning systems: Effects of individual and peer learning support. *Computers & Education, 57*(1), 1317-1333.

Chua, C., & Montalbo, J. (2014). Assessing Students' Satisfaction on the Use of Virtual Learning Environment (VLE): An Input to a Campus-wide E-learning Design and Implementation. In *Information and Knowledge Management, 4*(2), 108-115.

Cicchetti, D. V., Showalter, D., & Tyrer, P. J. (1985). The effect of number of rating scale categories on levels of interrater reliability: A monte carlo investigation. *Applied Psychological Measurement, 9*, 31-36.

Compeau, D., Marcolin, B., Kelley, H., & Higgins, C. (2012). Generalizability of information systems research using student subjects – a reflection of our practices and recommendations for future research. *Information Systems Research, 23*(4), 1093-1109.

Council, F. F. I. E. (2011). Authentication in an internet banking environment. Retrieved from *www.**ffiec**.gov/pdf/**authentication**_guidance.pdf.*

Crawford, C. M. (2001). Developing webs of significance through communications: Appropriate interactive activities for distributed learning environments. *Campus-Wide Information Systems, 18*(2), 68-72.

Cuillier, D. & Piotrowski, S. J. (2009). Internet information-seeking and its relations to support for access to government records. *Government Information Quarterly, 26*(3), 441-449.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-350.

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research, 3*(1), 60-95.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security, 7*(4), 171-175.

Dishaw, M. T., & Strong, D. M. (1999). Extending the technology acceptance model with *task–technology* fit constructs. *Information & Management, 36*(1), 9-21.

Dolnicar, S., & Grün, B. (2013). "Translating" between survey answer formats. *Journal of Business Research, 66*(9), 1298-1306.

El-Khatib, K., Korba, L., Xu, Y., & Yee, G. (2003). Privacy and security in e-learning. *International Journal of Distance Education Technologies, 1*(4), 1-19.

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology, 6*, 323-337.

Engeström, Y. (2001). Expansive learning at work: Towards an activity theoretical reconceptualization. *Journal of Education and Work, 14*(1), 133-156.

Eom, S., Ashill, N. J., Arbaugh, J. B., & Stapleton, J. L. (2012). The role of information technology in e-learning systems success. *Human Systems Management, 31*(3), 147-163.

Fenz, S., & Ekelhart, A. (2009). Formalizing information security knowledge. *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, 183-194.

Ferdousi, B., & Levy, Y. (2010). Development and validation of a model to investigate the impact of individual factors on instructors' intention to use e-learning systems. *Interdisciplinary Journal of E-Learning and Learning Objects, 6*, 1-21.

Flior, E., & Kowalski, K. (2010). Continuous biometric user authentication in online examinations. *Proceedings Seventh International Conference on Information Technology*, 488-492.

Frederickson, N., Reed, P., & Clifford, V. (2005). Evaluating web-supported learning versus lecture-based teaching: Quantitative and qualitative perspectives. *Higher Education, 50*(4), 645-664.

Fricker, S., Galesic, M., Tourangeau, R., & Yan, T. (2005). An experimental comparison of web and telephone surveys. *Public Opinion Quarterly, 69*(3), 370–393.

Fry, K. (2001). E-learning markets and providers: Some issues and prospects. *Education & Training, 43*(4/5), 233-239.

Furnell, S. (2007). An assessment of website password practices. *Computers & Security, 26*(7-8), 445-451.

Furnell, S. M., Dowland, P. S., Illingworth, H. M., & Reynolds, P. L. (2000). Authentication and supervision: A survey of user attitudes. *Computer & Security, 19*(6), 529–539.

Galanxhi, H., & Nah, F. F. (2007). Deception in cyberspace: A comparison of text-only vs. avatar-supported medium. *International Journal of Human-Computer Studies, 65*(9), 770-783.

Gao, Q. (2012). Using IP addresses as assisting tools to identify collusions. *International Journal of Business, Humanities and Technology, 2*(1), 70-75.

Gebauer, J., & Ginsburg, M. (2009). Exploring the black box of task-technology fit. *Communications of the ACM, 52*(1), 130-135.

Gibson, C. L., Khey, D., & Schreck, C. J. (2008). Gender, internal controls, and academic dishonesty: Investigating mediating and differential effects. *Journal of Criminal Justice Education, 9*(1), 2-18.

González, J. F., Rodríguez, M. C., Nistal, M. L., & Rifón, L. A. (2009). Reverse oauth: A solution to achieve delegated authorizations in single sign-on e-learning systems. *Computers & Security, 28*(8), 843-856.

Goodhue, D. (1988). I/S attitudes: Toward theoretical and definitional clarity. *ACM SIGMIS Database, 19*(3-4), 6-15.

Goodhue, D. L. (1998). Development and measurement validity of a task-technology fit instrument for user evaluations of information system. *Decision Sciences, 29*(1), 105-138.

Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quarterly*, 213-236.

Goodhue, D. L., Klein, B. D., & March, S. T. (2000). User evaluations of IS as surrogates for objective performance. *Information & Management, 38*(2), 87-101.

Graf, F. (2002). Providing security for e-learning. *Computers & Graphics, 26*(2), 355-365.

Green, M., & McGill, E. (2011). State of the Industry. ASTD's Annual Review of Workplace Learning and Development Data. ASTD Press, Alexandria, VA.

Gunasekaran, A., McNeil, R. D., & Shaul, D. (2002). E-learning: Research and applications. *Industrial and Commercial Training, 34*(2), 44-53.

Gupta, S., Cunningham, D. J., & Arya, A. (2009). A comparison of the ethics of business students: Stated behavior versus actual behavior. *Journal of Legal, Ethical and Regulatory Issues, 12*(2), 103-123.

Hasan, H., & Crawford, K. (2003). Codifying or enabling: The challenge of knowledge management systems. *The Journal of the Operational Research Society, 54*(2), 184-193.

Helkala, K., & Snekkenes, E. (2009). Formalizing the ranking of authentication products. *Information Management & Computer Security, 17*(1), 30-43.

Hernandez, J. A., Ortiz, A. O., Andaverde, J., & Burlak, G. (2008). Biometrics in online assessments: A study case in high school students. *Proceedings of the Eighteenth International Conference on Electronics, Communications and Computers*, 111-116.

Hollinger, R. C., & Lanza-Kaduce, L. (2009). Academic dishonesty and the perceived effectiveness of countermeasures: An empirical survey of cheating at a major public university. *NASPA Journal*, *46*(4), 587-602.

Howell, J., & Wei, J. (2010). Value increasing model in commercial e-banking. *The Journal of Computer Information Systems, 51*(1), 72-81.

Hsu, C., Lee, J. N., & Straub, D. (2012). Institutional influences on information systems security innovations. *Information Systems Research, 23*(2), 918-939.

Hutchinson, D., & Warren, M. (2003). Security for internet banking: a framework. *Logistics Information Management, 16*(1), 64-73.

Ibrahim, J., Ali, M. A., & Nassr, R. (2011). Using biometric techniques to secure online student assessment: Comparative study. *International Journal of Computer Science and Information Security, 9*(11), 41-43.

Inaba, R., Watanabe, E., & Kodate, K. (2003). Security applications of optical face recognition system: Access control in e-learning. *Optical Review, 10*(4), 255-261.

Jain, H., Ramamurthy, K., Hwa-Suk, R., & Yasai-Ardekani, M. (1998). Success of data resource management in distributed environments: An empirical investigation. *MIS Quarterly, 22*(1), 1-29.

Jalal, A., & Zeb, M. A. (2008). Security enhancement for e-learning portal. *International Journal of Computer Science and Network Security, 8*(3), 41-45.

Joint Information Systems Committee. (2006). E-assessment glossary (extended). Retrieved from http://www.jisc.ac.uk/uploaded_documents/eAssess-Glossary-Extended-v1-01.pdf.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kaplowitz, M. D., Hadlock, T. D., & Levine, R. (2004). A comparison of web and mail survey response rates. *Public Opinion Quarterly, 68*(1), 94-101.

Kasraie, N., & Kasraie, E. (2010). Economies of elearning in the 21st century. *Contemporary Issues in Education Research, 3*(10), 57-62.

Kerka, S., & Wonacott, M. (2000). *Assessing learners online*. ERIC, clearing house on adult, career and vocational education. Retrieve from http://www.eric.ed.gov/PDFS/ED448285.pdf.

Kim, J. J., & Hong, S. P. (2011). A method of risk assessment for multi-factor authentication. *Journal for Information Processing Systems, 7*(1), 187-198.

King, C. G., Guyette, R. W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business student's views. *The Journal of Educators Online, 6*(1), 1-11.

Kitahara, R., Westfall, F., & Mankelwicz, J. (2011). New, multi-faceted hybrid approaches to ensuring academic integrity. *Journal of Academic and Business Ethics, 3*(1), 1-12.

Kowalski, K., Wisniewski, W., & Beheshti, M. (2009). User's authentication in online examinations. *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications.* Chesapeake, VA: AACE, 1521-1526.

Kruck, S., & Teer, F. (2008). Computer security practices and perceptions of the next generation of corporate computer users. *International Journal of Information Security and Privacy, 2*(1), 80-90.

Lam, W. (2004). Encouraging online participation. *Journal of Information Systems Education, 15*(4), 345-349.

Lanier, M. M. (2006). Academic integrity and distance learning. *Journal of Criminal Justice Education, 17*(2), 244-268.

Lawrence, J. (2003). A distance learning approach to teaching management science and statistics. *International Transactions in Operational Research, 10*(2), 127-139.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2/3), 57-63.

Leedy, P. D., & Ormrod, J. E. (2010). *Practical research: Planning and design*. New York, NY: Merrill.

Levy, Y. (2003). A study of learner's perceived value and satisfaction for implied effectiveness of online learning systems. *Dissertation Abstracts International, A65*(03), 1014. (UMI No. AAT 3126765)

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

Levy, Y. (2006b). The top 10 most valuable online learning activities for graduate MIS students. *International Journal of Information and Communication Technology Education, 2*(3), 27–44.

Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education, 51*(4), 1664-1675.

Levy, Y., & Murphy, K. (2002). Toward a value framework for online learning systems. *Proceedings from Hawaii International Conference on System Sciences*.

Levy, Y., & Ramim, M. (2007). A theoretical approach for biometrics authentication of e-exams. *Chais Conference on Instructional Technologies Research, The Open University of Israel, Raanana, Israel.*

Levy, Y., & Ramim, M. (2009). Initial development of a learners' ratified acceptance of multibiometrics intentions model (RAMIM). *Interdisciplinary Journal of E-learning and Learning Objects, 5*(1), 379-397.

Levy, Y., & Ramim, M. (2010). Students' perceived ethical severity of e-learning security attacks. *Chais conference on Instructional Technologies Research, The Open University of Israel, Raanana, Israel.*

Levy, Y., Ramim, M. M., & Hackney, R. A. (2013). Assessing ethical severity of e-learning systems security attacks. *Journal of Computer Information Systems, 53*(3).

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.

Lin, W. S. (2012). Perceived fit and satisfaction on web learning performance: IS continuance intention and task-technology fit perspectives. *International Journal of Human-Computer Studies, 70*(7), 498-507.

Liou, J., & Bhashyam, S. (2010). On improving feasibility and security measures of online authentication. *International Journal of Advancements in Computing Technology, 2*(4), 1-11.

Liu, X., & Schwen, T. M. (2006). Sociocultural factors affecting the success of an online MBA course. *Performance Improvement Quarterly, 19*(2), 69-92.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly, 35*(2), 293-334.

Makransky, G., & Glas, C. A. (2011). Unproctored internet test verification: Using adaptive confirmation testing. *Organizational Research Methods, 14*(4), 608-630.

Marais, E., Argles, D., & Von Solms, S. H. (2006) Security issues specific to e-assessments. *Proceedings of the 8th Annual Conference on WWW Applications.*

Masters, K., & Ellaway, R. (2008). E-Learning in medical education guide 32 Part 2: Technology, management and design. *Medical Teacher, 30*(5), 474-489.

McGill, T. J., & Klobas, J. E. (2009). A task-technology fit view of learning management system impact. *Computers & Education, 52*(2), 496-508.

Mertler, C. A., & Vannatta, R. A. (2010). *Advanced and multivariate statistical methods*. Glendale, CA: Pyrczak.

Moini, A., & Madni, A. M. (2009). Leveraging biometrics for user authentication in online learning: A systems perspective. *IEEE Systems Journal, 3*(4), 469-476.

Moore, G., & Benbasat, I. 1991. Development of an instrument to measure perceptions of adopting an information technology innovation. *Information Systems Research, 2*(3), 192–222.

Newsom, J. (2005). *A quick primer on exploratory factor analysis*. Retrieved from http://www.upa.pdx.edu/IOA/newsom/semclass/ho_efa.doc.

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), 2019-2040.

Oakley, R. L., & Singh, R. (2011). Ethical decision-making in e-learning: A socio-technical analysis of informal security controls. *Proceedings Americas Conference on Information Systems, 455,* 1-8.

Okoli, C., & Pawlowski, S. D. (2004). The delphi method as a research tool: An example, design considerations and applications. *Information & management, 42*(1), 15-29.

Ong, C. S., & Lai, J. Y. (2006). Gender differences in perceptions and relationships among dominants of e-learning acceptance. *Computers in Human Behavior*, *22*(5), 816-829.

Ossiannilsson, E., & Landgren, L. (2012). Quality in e-learning–a conceptual framework based on experiences from three international benchmarking projects. *Journal of Computer assisted learning, 28*(1), 42-51.

Park, J., & Wentling, T. (2007). Factors associated with transfer of training in workplace e-learning. *Journal of Workplace Learning, 19*(5), 311-329.

Passow, H. J., Mayhew, M. J., Finelli, C. J., Harding, T. S., & Carpenter, D. D. (2006). Factors influencing engineering students' decisions to cheat by type of assessment. *Research in Higher Education, 47*(6), 643–684.

Penteado, B. E., & Marana, A. N. (2009). A video-based biometric authentication for e-learning web applications. *Enterprise Information Systems, (24)*4, 770-779.

Peslak, A. R. (2008). Current information technology issues and moral intensity influences. *The Journal of Computer Information Systems, 48*(4), 77-86.

Prince, D. J., Fulton, R. A., & Garsombke, T. W. (2009). Comparisons of proctored versus non-proctored testing strategies in graduate distance education curriculum. *Journal of College Teaching and Learning, 6*(7), 51-62.

Rabuzin, K., Bača, M., & Sajko, M. (2006). E-learning: Biometrics as a security factor. *Proceedings in International Multi-Conference on Computing in the Global Information Technology*, 61-64.

Rathgeb, C., & Uhl, A. (2010). Two-factor authentication or how to potentially counterfeit experimental results in biometric systems. *Proceedings of the International Conference on Image Analysis and Recognition*, 296-305.

Rodchua, S., Yiadom-Boakye, G., & Woolsey, R. (2011). Student verification system for online assessments: Bolstering quality and integrity of distance learning. *Journal of Industrial Technology, 27*(3), 1-8.

Rovai, A. P. (2000). Online and traditional assessments: What is the difference? *The Internet and Higher Education, 3*(3), 141-151.

Rowe, N. C. (2004). Cheating in online student assessment: Beyond plagiarism. *Online Journal of Distance Learning Administration, 7*(3).

Roy, A., & Raymond, L. (2008). Meeting the training needs of SMEs: Is e-learning a solution. *The Electronic Journal of e-Learning*, *6*(2), 89-98.

Sadler, R. (1989). Formative assessment and the design of instructional systems. *Instructional Science, 18*(2), 119-144.

Schmelkin, L. P., Gilbert, K., Spencer, K. J., Pincus, H. S., & Silva, R. (2008). A multidimensional scaling of college students' perceptions of academic dishonesty. *Journal of Higher Education, 79*(5), 587-607.

Schneier, B. (2005). Two-factor authentication: Too little, too late. *Communications of ACM, 48*(4), 136.

Sekaran, U. (2003). *Research methods for business - A skill building approach*. New York, NY: Wiley & Sons.

Selim, H. M. (2007). Critical success factors for e-learning acceptance: Confirmatory factor models. *Computers & Education, 49*(2), 396-413.

Sheenhan, K. B. (2001). E-mail survey response rates: A review. *Journal of Computer-Mediated Communication, 6*(2).

Sills, S. J., & Song, C. (2002). Innovations in survey research: An application of web surveys. *Social Science Computer Review, 20*, 22-30.

Simon, J. C., & Chaney, L. H. (2006). Trends in students perceptions of the ethicality of selected computer activities. *Academy of Educational Leadership Journal, 10*(1), 1-9.

Stanton, J. M., & Rogelberg, S. G. (2001). Using internet/intranet web pages to collect organizational research data. *Organizational Research Methods, 4*(3), 200-217.

Staples, D. S., & Seddon, P. (2004). Testing the technology-to-performance chain model. *Journal of Organizational and End User Computing, 16*(4), 17-36.

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

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-60.

Suqrue, B., & Rivera, R. J. (2005). State of the Industry Report, ASTD Press, Alexandria, VA.

Suri, G., & Sharma, S. (2013). The impact of gender on attitude towards computer technology and e-learning: An exploratory study of Punjab University, India. *International Journal of Engineering Research*, *2*(2), 132-136.

Van Aken, J. E. (1978). *On the control of complex industrial organizations.* London: Martin us Nijhoff Social Sciences Division.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioral compliance. *Computers & Security, 23*(3), 191-198.

Walker, K. (2004). Activity systems and conflict resolution in an online professional communication course. *Business Communication Quarterly, 67*(2), 182-197.

Wang, M., Ran, W., Liao, J., & Yang, S. J. (2010). A performance-oriented approach to e-learning in the workplace. *Educational Technology & Society, 13*(4), 167-179.

Wang, Y. S., Wang, H. Y., & Shee, D. Y. (2007). Measuring e-learning systems success in an organizational context: Scale development and validation. *Computers in Human Behavior*, *23*(4), 1792-1808.

Weippl, E. R. (2005). *Security in E-Learning (Advances in Information Security).* New York: Springer-Verlag.

Welsh, E. T., Wanberg, C. R., Brown, K. G., & Simmering, M. J. (2003). E-learning: emerging uses, empirical results and future directions. *International Journal of Training and Development*, *7*(4), 245-258.

Yang, Y., & Padmanabhan, B. (2010). Toward user patterns for online security: Observation time and online user identification. *Decision Support Systems, 48*(4), 548-558.

Yoon, Y., Guimaraes, T., & O'Neal, Q. (1995). Exploring the factors associated with expert systems success. *MIS Quarterly, 19*(1), 83-106.

Yu, T. K., & Yu, T. Y. (2010). Modelling the factors that affect individuals' utilisation of online learning systems: An empirical study combining the task technology fit model with the theory of planned behaviour. *British Journal of Educational Technology, 41*(6), 1003-1017.

Zviran, M., & Erlich, Z. (2006). Identification and authentication: Technology and implementation issues. *Communications of the Association for Information Systems 17*(1), 90-105.