
Electronic Theses and Dissertations, 2004-2019

2011

Testing The Impact Of Training With Simulated Scenarios For Information Security Awareness On Virtual Community Of Practice Members

Craig Leonard Tidwell
University of Central Florida



Part of the [Engineering Commons](#)

Find similar works at: <https://stars.library.ucf.edu/etd>

University of Central Florida Libraries <http://library.ucf.edu>

This Doctoral Dissertation (Open Access) is brought to you for free and open access by STARS. It has been accepted for inclusion in Electronic Theses and Dissertations, 2004-2019 by an authorized administrator of STARS. For more information, please contact STARS@ucf.edu.

STARS Citation

Tidwell, Craig Leonard, "Testing The Impact Of Training With Simulated Scenarios For Information Security Awareness On Virtual Community Of Practice Members" (2011). *Electronic Theses and Dissertations, 2004-2019*. 1980.

<https://stars.library.ucf.edu/etd/1980>

**TESTING THE IMPACT OF TRAINING WITH SIMULATED SCENARIOS FOR
INFORMATION SECURITY AWARENESS ON VIRTUAL COMMUNITY OF
PRACTICE MEMBERS**

by

CRAIG LEONARD TIDWELL
M.S. University of Central Florida, 2006
M.S. University of North Carolina, 1991
B.S. California State University, 1985

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in Modeling and Simulation
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Spring Term

2011

Major Professor: Charles Reilly

© Craig Leonard Tidwell

ABSTRACT

Information security has become a major challenge for all private and public organizations. The protection of proprietary and secret data and the proper awareness of what is entailed in protecting this data are necessary in all organizations. This treatise examines how simulation and training would influence information security awareness over time in virtual communities of practice under a variety of security threats. The hypothesis of the study was that security-trained members of a virtual community of practice would respond significantly better to routine security processes and attempts to breach security or to violate the security policy of their organization or of their virtual community of practice.

Deterrence theory was used as the grounded theory and integrated in the information security awareness training with simulated scenarios. The study provided training with simulated scenarios and then tested the users of a virtual community of practice over an approximately twelve-week period to see if the planned security awareness training with simulated security problem scenarios would be effective in improving their responses to the follow-up tests.

The research subjects were divided into four groups, the experimental group and three control groups. The experimental group received all of the training and testing events throughout the twelve-week period. The three control groups received various portions of the training and testing. The data from all of the tests were analyzed using the Kruskal-Wallis

ranked order test, and it was determined that there was no significant difference between the groups at the end of the data collection.

Even though the null hypothesis, which stated that there would be no difference between the groups scores on the information security awareness tests, was not rejected, the groups that received the initial training with the simulated scenarios did perform slightly better from the pre-training test to the post-training test when compared with the control group that did not receive the initial training.

More research is suggested to determine how information security awareness training with simulated scenarios and follow-up testing can be used to improve and sustain the security practices of members of virtual communities of practice. Specifically, additional research could include: comparing the effect of training with the simulated scenarios and with training that would not use the simulated security scenarios; the potential benefits of using adaptive and intelligent training to focus on the individual subjects' weaknesses and strengths; the length of the training with simulated scenarios events, the time between each training event, and the overall length of the training; the demographics of the groups used in the training, and how different user characteristics impact the efficacy of the training with simulated scenarios and testing; and lastly examining how increasing the fidelity of the simulated scenarios might impact the results of the follow-up tests.

TABLE OF CONTENTS

LIST OF FIGURES.....	viii
LIST OF TABLES.....	x
LIST OF ACRONYMS/ABBREVIATIONS.....	xii
CHAPTER ONE: INTRODUCTION.....	1
Overview	1
Conceptual Underpinnings for the Study.....	7
Statement of the Problem.....	8
Purpose of the Study.....	9
Outline of Treatise.....	10
CHAPTER TWO: LITERATURE REVIEW	11
Introduction.....	11
Communities of Practice	12
Virtual Communities of Practice	16
Deterrence Theory	18
Information Security (InfoSec)	21
Points and Causes of Security Breaches	26
Hackers Geographic Location and International Issues.....	30
Cost of Security Breaches	31
Security Awareness and Training.....	32
Ways to Avoid Data Compromises (Breaches)	34
Threats to Confidentiality	38
Providing Access	38
Information Security Policies	40
Simulation and Training in Computer Security	46
Taxonomy of Computer Security Incidents.....	48
Summary	51

CHAPTER THREE: METHODOLOGY	53
Introduction.....	53
Research Study	55
Research Questions and Hypothesis.....	63
Data Collection and Instrumentation.....	65
Data Analysis	67
Summary	71
CHAPTER FOUR: ANALYSIS OF DATA	73
Introduction.....	73
Organization of Data Analysis	74
Presentation of Descriptive Characteristics of Respondents.....	74
Pilot Study	74
Full Research Study	77
Demographic Data	77
Research Questions and Associated Hypotheses	80
Data Collection Process.....	81
Analysis of Data	108
CHAPTER FIVE: FINDINGS, CONCLUSIONS, AND FUTURE RESEARCH	124
Recap of the Study	124
Findings	125
Future Research	136
APPENDIX A: DEMOGRAPHIC SURVEY	140
APPENDIX B: TESTS TAKEN BY RESEARCH SUBJECTS	142
Pre-Training Test and Final Test.....	143
Post-Training Test.....	147
Week 3 Follow-Up Test	151
Week 6 Follow-Up Test	153
Week 9 Follow-Up Test	155

APPENDIX C: DATA COLLECTED DURING RESEARCH STUDY.....	157
APPENDIX D: SIMULATED DATA FOR TESTING KRUSKAL-WALLIS STATISTICAL ANALYSIS	162
APPENDIX E: TRAINING SYLLABUS	168
APPENDIX F: SAMPLES OF TRAINING WITH SIMULATED SCENARIOS AND TESTING EVENTS	176
APPENDIX G: POTENTIAL INTERVIEW QUESTIONS	181
APPENDIX H: IRB INFORMED CONSENT	183
LIST OF REFERENCES	189

LIST OF FIGURES

Figure 1 – Initial Login Screen for All Groups.....	82
Figure 2 – Demographic Survey Screen	83
Figure 3 – Screen after Demographic Survey Completion.....	84
Figure 4 – Pre-training Test Screen.....	85
Figure 5 – Initial Security Training Introduction Screen	86
Figure 6 – Initial Training Overview Screen 1	86
Figure 7 – Initial Training Overview Screen 2	87
Figure 8 – Initial Training Part I.....	88
Figure 9 – Password Checking Site.....	88
Figure 10 – Initial Training Part II.....	89
Figure 11 – File Sharing Simulation.....	90
Figure 12 – Email Simulation	90
Figure 13 – Initial Training Part III.....	92
Figure 14 – Virus Simulation Screen	92
Figure 15 – Phishing Simulation Screen.....	93
Figure 16 – Initial Training Part IV.....	94
Figure 17 – Social Engineering Screen	95
Figure 18 – Initial Training Conclusion Screen.....	95
Figure 19 – Post-training Test Initial Screen	96
Figure 20 – Post-training Test Screen	97
Figure 21 – Post-training Test Conclusion Screen	97
Figure 22 - Follow Up Training - Week 3 Screen (page 1).....	99
Figure 23 - Follow Up Training - Week 3 Simulation Screen.....	99
Figure 24 - Follow Up Training - Week 3 Test Screen	100
Figure 25 - Follow Up Training - Week 3 Conclusion Screen	100
Figure 26 - Follow Up Training - Week 6 Screen (page 1).....	102

Figure 27 - Follow Up Training - Week 6 Simulation Screen.....	102
Figure 28 - Follow Up Training - Week 6 Test Screen	103
Figure 29 - Follow Up Training - Week 6 Conclusion Screen	103
Figure 30 - Follow Up Training - Week 9 Screen (page 1).....	104
Figure 31 - Follow Up Training - Week 9 Simulation Screen.....	105
Figure 32 - Follow Up Training - Week 9 Test Screen	105
Figure 33 - Follow Up Training - Week 9 Conclusion Screen	106
Figure 34 - Final Test Introduction Screen.....	107
Figure 35 - Final Test Screen	107
Figure 36 - Final Test Conclusion Screen	108
Figure 37 - Bar Chart of Test Score Data.....	127
Figure 38 - Line Graph of Group A Data.....	129
Figure 39 - Line Graph of Group B Data.....	130
Figure 40 - Line Graph of Group C Data	131
Figure 41 – Groups A, B, and C Test Scores	132
Figure 42 – Simulated Example Event.....	174
Figure 43 – Sample Email Simulated Event.....	177
Figure 44 – Sample Potential Virus File	179
Figure 45 – Sample Password Simulation	180

LIST OF TABLES

Table 1 - A New Taxonomy (Kjaerland, 2006)	49
Table 2 - Timeline and Events for Research Study.....	56
Table 3 - Topics to be Included in the Computer Security Tutorial	61
Table 4 - Data Collected and Data Collection Points	66
Table 5 - Pilot Test Time Line and Events	68
Table 6 - Number of Subjects in Each Group for the Full Research Study	69
Table 7 - Pilot Study Data.....	76
Table 8 - Demographic Data by Groups.....	78
Table 9 - Pre-training Test Summary Data	109
Table 10 - Pre-training Test Kruskal Wallis Test Results	110
Table 11 - Post-training Test Summary Data	111
Table 12 - Kruskal Wallis Post-Training Test Results at 5%	112
Table 13 - Kruskal Wallis Post-Training Test Results at 10%	113
Table 14 - Pre and Post-training Test Scores	113
Table 15 - Follow-Up Testing Data, Week 3.....	114
Table 16 - Week 3 Follow-Up Test Results.....	115
Table 17 - Follow-Up Testing Data, Week 6.....	116
Table 18 - Week 6 Follow-Up Test Results.....	117
Table 19 - Week 3 and Week 6 Test Results.....	117
Table 20 - Follow-Up Testing Data, Week 9.....	118
Table 21 - Week 9 Follow-Up Test Results.....	119
Table 22 - Week 3, 6, and 9 Summary Data Statistics	119
Table 23 - Final Test Summary Results	121
Table 24 - Final Test Results.....	122
Table 25 - Final Comparison of Groups.....	123

Table 26 – Confidence Intervals at 95%.....	128
Table 27 - Mean Scores for All Groups and All Tests	134
Table 28 – Pre-Training Test Data.....	158
Table 29 – Post-Training Test Data	159
Table 30 – Final Test Data	160
Table 31 – Computed Confidence Intervals for Test Means	161
Table 32 – Sample Data for Testing Kruskal-Wallis	163
Table 33 - Means by Question from Each Group in Simulated Data	165
Table 34 - Ranking of Means from Simulated Data for Kruskal-Wallis Test	165
Table 35 – Simulated data results using PhStat2.....	167
Table 36 - Maximum Estimated Training with simulated scenarios and Testing Time	175

LIST OF ACRONYMS/ABBREVIATIONS

ACL – Access Control List

AICPA - American Institute of Certified Public Accountants

CAS - Community Authorization Service

CDI – Constrained Data Items

CERT - Computer Emergency Response Team

CISR - Center for the Information Systems Studies and Research

COM – Commercial

COP – Community of Practice

CSI – Computer Security Institute

DAC - Discretionary Access Control

DNS – Domain Name System

DOS – Denial of Service

EDI – Electronic Data Interchange

FBI – Federal Bureau of Investigation

GOV – Government

InfoSec – Information Security

IPSec – Internet Protocol Security

IS – Information Systems

ISAC - Information Sharing and Analysis Center

IT – Information Technology

LAN – Local Area Network

MAC - Mandatory Access Control

OS – Operating System

RINSE - Real-Time Immersive Network Simulation Environment

SAIC - Science Applications International Corporation

SANS - System Administration, Networking, and Security Institute

UDI – Unconstrained Data Items

V-CoP – Virtual Community of Practice

CHAPTER ONE: INTRODUCTION

Overview

We live in an information age that is dominated by online communications through such mechanisms as online affinity and network groups (e.g. Facebook, MySpace, Twitter, etc.), virtual online communities of practice, virtual worlds (e.g. Second Life), and other computer-enabled mediation of knowledge sharing (Wikis, Blogs, etc.). This treatise focuses on using information security awareness training with simulated security events within a virtual community of practice (V-CoP). Information security training includes areas such as password security and maintenance, data sharing, computer viruses, and how careless information security practices are responsible for massive data losses and an untold number of employee work hours in repairing the damages. For example, in 2003 alone computer viruses cost companies an estimated \$45 billion (Kjaerland, 2006).

Virtual communities exchange massive amounts of data that needs to be managed and stored in a secure manner, which poses a predicament for any organization. On one hand, these groups are being leveraged as a new medium for intra- and inter-organizational knowledge sharing, and on the other hand, there has never been a larger group of potential computer hackers waiting to take advantage of this new target-rich virtual environment. Connections to organized crime have been made by the FBI for some of the illicit hacking that is taking place (Richardson, 2008). Communication and sharing of knowledge and data are being handled by many companies through virtual communities that link people together from all

parts of the globe, which results in information security challenges that are not necessarily found in traditional non-virtual groups.

Balancing the necessity to share information and to control access to this same information has been and will continue to be a challenge among the world's businesses, government agencies, and other organizations. These companies and organizations collect and store a vast quantity of data about their customers, products, employees, and partners. These data must be safeguarded and yet still be made available. Cost is the driving factor in this battle, and organizations must balance the costs of securing these data with the costs of losing access to and possession of their information in both quantitative and qualitative terms.

It is difficult to assign specific financial costs to information, but much of the data that is collected and stored by organizations is its lifeblood, and proper protection and security is critical to ensure its continuity and accuracy. A study conducted by the McAfee Corporation projected that companies worldwide lost more than \$1 trillion to computer security breaches in 2008 alone (Knights, 2009). The problem of losses due to hacking has been exacerbated by the recent economic downturn, and the study reports that two out of five organizations surveyed were now more vulnerable to breaches. Furthermore, Forrester Research estimates that an average computer security breach can cost a company between \$90 and \$305 per record (Gaudin, 2007). Since most breaches do not just involve tens or even hundreds of records, but rather hundreds of thousands or even millions of records, the cost of the breach and the cost of repair can be in the millions of dollars. For example, TJX Companies Inc. was hacked in 2007 and a reported 46 to 215 million customer records were stolen (Hakala, 2008). So the cost to

TJX could be as high as \$65 billion (215 million records at \$305 per record). Questions arise about the causes and remedies of these breaches. In this virtual world of computer transactions, how does an organization adequately protect its valuable information assets?

Organizations all over the world need to learn how to create and implement information security policies and procedures to protect organizational data and to make sure that their employees are not only aware of these policies but that employees are tested on the contents of these policies as part of an ongoing process to ensure that they do not unnecessarily open themselves up to attack. Security issues are particularly challenging in a V-CoP, where members may be internal employees, external partners, the general public, and even competitors. Users are a large cause of security problems within organizations, and the major cause of most of the worst breaches in 2007 was not from outside hackers, but rather from employees' carelessness (Hakala, 2008).

Furthermore, a large number of information security breaches are caused by human error or human failure when employees do not follow specified information security practices. Human error represents a significant threat, requiring the implementation of controls to reduce the frequency and severity of such mistakes (Whitman, 2004). Lastly, when companies do not meet the specified requirements for data security, whether that shortcoming is willful or negligent, they have failed in their obligations to their stakeholders (Wilson, 2009). Not only is the organization liable to its own internal users, but it is also liable to those parties with a financial interest (e.g. stockholders).

Key to this problem is awareness of security risks and the necessary education and training about information security. Organizations need to increase employee training and awareness to avoid accidental and careless mistakes and to increase the effectiveness of their security policies (Whitman, 2004). Information security awareness can be described as the state where users are aware of, or attentive to, their security mission as expressed in end-user guidelines or the security policy (Siponen, 2000). In the 2009 Computer Security Institute's (CSI)/Federal Bureau of Investigation (FBI) survey, 53 percent of the respondents said that their organizations allocate 5 percent or less of their overall IT budget to information security. In addition, 42 percent spend less than 1 percent of their security dollars on awareness programs, which is an alarmingly low expenditure rate when one considers the cost of dealing with security breaches (Richardson, 2008). The fact that approximately \$0.50 for every \$1,000 is spent on information security reveals the need for more focus on awareness education, training, and continuous and random follow-up testing.

One way to solve the cost issue can be through the use of simulation. Simulation can be a cost-effective way to implement a solution to end-user training in proper computer security practices. Included in this training with simulated scenarios would be a proper understanding of the common security policies that are part of the company's standard operating procedures, the dangers of not adhering to good security practices, and scenarios that test the users' understanding of the information security topics presented. Simulation has been effectively used in other areas such as automobile traffic routing and design and in the education field through simulated labs and experiments. Simulation has been used by almost

every other sector of society to train employees and to test solutions before they are implemented.

Information security starts with the policies and procedures that an organization adopts for protecting their valuable data. According to Whitman, a security policy is the single most important issue for protecting a computer system or network from hackers (Whitman, 2004). Also, Sword and Shield Security Consultants (2001) found that implementation of a security policy is the number one recommended action for protecting an organization's IT systems. The policy should outline both individual and corporate responsibilities, define authorized and unauthorized use of systems, report threats and breaches, and define penalties for violating the policy. The policy should also include a method for updating the policy. Key to these policies is the balance of providing confidentiality, integrity, and availability (Blake, 2000). The cornerstone of the information security policy is ensuring that data is kept private (confidentiality), that the data can be relied upon to be accurate (integrity), and accessible only by authorized (and authenticated) individuals in a timely and available manner. Security policies have long been seen as the key to identifying and managing the security threats and the resources needed to secure information and the systems that hold that data (Anderson, 1996).

In a virtual environment, security poses a serious challenge as part of the problem is the enormous amount of data that is available. Proper utilization and assimilation of collected data can be accomplished through the informal and formal organization of employees in virtual groups that are connected through a shared practice. Such a group, as coined by Wenger and

Lave (Wenger, 1999), is called a community of practice (CoP). A CoP is a group of people informally bound together by some shared passion for a joint enterprise (Wenger & Snyder, 2000). A V-CoP is a CoP that is convened and meets in a virtual environment where members may never meet in person.

Ultimately what is needed is a new model that incorporates the nuances from a V-CoP where the boundaries, topics of discussion, and membership of the CoP may change on a daily basis (Wenger, 2000). A new model would include a comprehensive security awareness program that incorporates initial training for individuals that are members of a V-CoP and ongoing monitoring and periodic testing. Included with the random testing of members of the V-CoP will be mock security incident testing (Baker, 2008) to make sure that the members are adhering to the security policy they agreed to, are educated about, and are tested on (see Appendix E for a training syllabus). Part of this process is to educate the members of the V-CoP on the potential threats and damages that can be caused by careless behavior that compromises computer security and may lead to financial and other losses.

The simulated mock security events would be part of the training and consist of a simulated security incident, such as a counterfeit email, which asks the member of the V-CoP to reveal confidential data or other proprietary information within the safety of a designed simulated security event. The member then would have to properly respond to the simulated scenario within the web-based environment. This simulated mock security incident would be a planned part of the initial training and then would consist of follow-up training events that would occur periodically on an ongoing basis to test the end-users' awareness of the security

policy. If they do not respond appropriately to subsequent events, they will be presented with follow-up training tips via the web portal to remind them of the proper application of a typical security policy. A sufficient passing rate would be determined by the type of organization that the end-user works for and the level of data access associated with the end-user. For example, in a classified environment like military intelligence or the research and development department of a corporation, the passing rate may be 100%. However, in another environment where the data is not as sensitive, the passing rate could be lower.

Conceptual Underpinnings for the Study

The theoretical basis for this study is deterrence theory. Originally coined from the cold war era of potential mutual destruction between the US and the USSR, the theory is based upon the premise that one party will not engage in aggressive behavior if the opponent has the ability and will to retaliate with the same or superior force, and it should include the understanding of what an adversary values (Nautilus, 1995). Since its original application to nuclear deterrence, scholars have applied the theory to the prevention of criminal activity. If an organization understands what an adversary values (e.g. financial data, or any data that can easily be turned into monetary gain), then it can spend more of its limited resources on protecting those assets, and if the adversary perceives a high likelihood of detection and capture, then the probability of the attack should diminish.

The focus of this research is on how deterrence theory can be applied to information security by properly educating V-CoP participants on the destruction and harm that computer hackers can cause by the lack of end-user adherence to standard computer security policy practices.

Statement of the Problem

While much has been done in the field of computer security and in determining different ways to deter information system abuse, the application of deterrence theory to V-CoPs has not been explored. Users are usually unaware of the risks of careless or reckless behaviors and their negative impact on information security. Members of a V-CoP must be aware of not only the type and sensitivity of the data they are posting or discussing in an online forum, but they need to be able to identify the recipient on the other end, or at least have an understanding about what type of access is enforced throughout the network of the V-CoP. End users must be properly trained and educated on security awareness practices since they are the major problem in information security for any organization.

Purpose of the Study

The purpose of this study was to determine if security awareness training with simulated security events and follow-up testing would have a positive effect on the members of a V-CoP.

Four groups were used in the study, three control groups (labeled B, C, and D), and one experimental group (labeled A). Groups A, B, and C received a pre-training test to check their knowledge and understanding of normal security procedures; Group D did not. Group B received no advanced security awareness training but was presented with the mock simulated security scenarios with follow-up testing to measure their responses to the training. Control Group C received the initial training but did not receive any follow-up training. Group A and control Group C received the security awareness training, approximately one to two weeks after the pre-training test and then were presented with the mock security scenarios and testing (see Appendix F for examples of the simulated security scenarios). Groups A and B were evaluated on their responses to the security scenarios. Approximately 3, 6, and 9 weeks after the initial training and test, Groups A and B were presented with another training event with a simulated security scenario and were then tested and their responses were measured and recorded. The responses were then compared with the responses recorded in the initial pre-training test and post-training test. At approximately 12 weeks a final test was delivered to all four groups that was identical to the pre-training test. The hypothesis was that the users who received the training with simulated security events would have a higher score on the post-

training test versus the pre-training test. It was also hypothesized that the subjects who did not receive the training would have similar scores on the pre- and post-training tests. Follow-up interviews were considered but not warranted based on the homogeneity of the groups involved in the study. Data gathered from the tests and events may be presented to the institutions involved to provide feedback on how they may need to change their security policy and procedures.

Outline of Treatise

Chapter 2 includes a comprehensive literature. How the experiment was designed, what methodology was used, and what data was collected was discussed in Chapter 3. The data collection methods and the statistical results are presented in Chapter 4. Chapter 5 presents conclusions, recommendations and observations related to future study and research.

CHAPTER TWO: LITERATURE REVIEW

Introduction

Information security in V-CoPs has been largely ignored. Members of a V-CoP must rely on the protections that have been implemented and assume that these protections are sufficient. However, many users do not even consider the proprietary nature of the data and information that they are sharing, nor are they sure of who is at the other end of the communication channel. Understanding computer security is important, but most users do not have the time or the inclination to learn or keep up to date. Lack of security awareness is a troubling problem as end-users are the primary cause of most computer breaches (Hakala, 2008). Even though end-users are the major cause of information security breaches, proper security controls accompanied by security awareness education can help to diminish this trend (Whitman, 2004).

Through security awareness education/training, through the application of deterrence theory, the members of a V-CoP will not only be more aware of information security issues, but they will be more likely to spot a potential security breach. Through deterrence theory application, members will be educated on the potential damage that can be done by a malicious hacker and the substantial costs. Also, members will be made aware of common techniques and issues in information security.

This chapter examines CoPs and V-CoPs. Research in these areas is examined with a focus on information security. Next, information security and information security breaches are discussed. Lastly, information security policies, taxonomy of security breaches, and computer security awareness training are discussed.

Communities of Practice

According to Wenger, “communities of practice are groups of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly”, (Wenger, 1999). They are formed by people who “engage in a process of collective learning in a shared domain of human endeavor” (Wenger, 1999). Some of the unique features of CoPs are their self-organizing nature and how they can spontaneously appear almost anywhere and in almost any format (Sharratt, 2003). CoPs have been around as long as humans have learned together and can be found in almost every discipline. Most recently, the concept has been adopted by business due to the valuable nature of knowledge and information. Any group that seeks to learn within a shared domain (accounting, supply chain management, fishing techniques, etc.) can therefore be considered to be a CoP (Barth, 2004). According to Wenger, there are three components that constitute a CoP, and these three components are developed in parallel (Wenger, 1999). They are the domain, the community, and the practice.

- The domain is the “shared domain of interest” of the group of people that are involved. A member of a CoP implies a certain level of commitment and competence to the domain. This distinguishes members of the CoP over others that may or may not be part of the domain.
- The community is the group of people who interact and learn from each other. They engage in joint activities and discussions, help each other, and share information. They may or may not work together on a daily basis, they are geographically dispersed or even work for different organizations.
- The practice is a developed set of stories and cases, a shared repertoire that is used in a CoP. The “practice” takes time and sustained interaction between the members. The development of a shared practice may be intentional or unintentional.

CoPs can be classified into four different models. They can be internal CoPs, CoPs in network organizations, formal networks of practice, and self-organizing networks of practice (Coakes, 2005). Internal CoPs are entirely within individual organizations. For example, IBM’s Global Services organization has over 60 CoPs with a total of 20,000 members across most of the countries that it serves. These communities handle explicit knowledge, adopt roles for handling this knowledge, and provide opportunities for sharing tacit knowledge (Coakes, 2005).

A network organization is a relationship between independent organizations (Powell, 1990). An example of this type of network is a supply chain. Members of these organizations work in close and ongoing cooperation on projects or processes (Coakes, 2005). The problem with this type of network is there is always the risk of knowledge leakage, which is an obvious security issue (Sampson, 2004).

Networks of practice are extra-organizational CoPs that are focused on work practice primarily through electronic communication. Network CoPs can be useful for solving problems in a certain discipline across organizations. However, this model can also have issues with security issues related to proprietary knowledge.

Lastly, a self-organizing network of practice is a loosely organized and informal network that has no central authority, and membership is voluntary.

CoPs are valuable to organizations since knowledge has long been recognized as a valuable resource for growth and competitive advantage (Johnson, 2001; Sharratt, 2003; Wasko, 2005; Wenger, 2003). A main reason for the increase in interest in CoPs is dissatisfaction with traditional learning methods and arenas (Johnson, 2001). The successes of today's organizations depend not on a divide and conquer strategy, but rather on sharing knowledge, which is the purpose of a CoP (Neus, 2001). The more that knowledge exchange can properly occur within an organization, the more efficient the organization can be. Knowledge exchange can also diminish the loss of information through employee attrition (Wenger, 2004). As employees share knowledge with others, new knowledge is created and added to the knowledge repository of the organization. This knowledge is collected and becomes part of the knowledge base of the organization. These knowledge bases are managed by knowledge management systems.

Knowledge management is the systematic approach for sustainably improving the handling of knowledge on all levels of an organization in order to support the organization's business goals, such as innovation, quality, cost effectiveness, etc (Boella, and van der Torre,

2006). Knowledge is the result of different perspectives and partial interpretations of world portions or domains, called the subjectivity and sociality of knowledge, and therefore, it should not be viewed as an absolute monolithic matter, but as a “system of local ‘knowledges’ continuously negotiated by communities of ‘knowers’” (Boella, and van der Torre, 2006).

Knowledge management systems (KMS) have been touted as critical tools for sharing of information, and in an ideal setting, this would be true. Knowledge by itself that is transferred solely through electronic reproduction can fall short of its potential if the knowledge is not placed in context and if employees do not know the “story” behind the knowledge (Wasko, 2005; Wenger, 2004). Organizations must also realize that this knowledge is not just a group of facts that appear in a spreadsheet or other explicit knowledge which is easier to transmit but more difficult to safeguard (Coakes, 2005). Knowledge, to a large extent, is embedded in individuals. It is inseparable from people in its fullest and most valuable form when it can be placed in context, exchanged in a meaningful way, clarified as needed, and applied in a useful method (Wasko, 2005). Extended even further, when knowledge is managed and shared within a community that knowledge supersedes the individual (Wenger, 1999). Transfer of tacit knowledge is critical to an organization and requires that an individual passes on this knowledge in context, and with relevant historical background (how was the knowledge acquired, from where, etc.) (Ardichvili, 2003; Wasko and Faraj 2005; Wenger, 2003; Sharratt, 2003).

How do organizations get employees to share their knowledge in a community, particularly when it is done over communication systems like the internet? Wasko and Faraj

(2005) found that people participate primarily out of “community interest, generalized reciprocity, and pro-social behavior”. Another study found that V-CoP members’ willingness to share are based on factors such as ease of use and perceived usefulness of the knowledge management system, trust (how well does one member trust the other members), perceived proximity of knowledge sharing to career advancement, sense of community, and perceived value congruence (Sharratt, 2003). Lastly, members of CoPs have been found to share when they perceive that it will enhance their professional reputation, when they have the experience to share, and when they are part of the network of members (Wasko and Faraj, 2005). As trust is a major contributor to “sharing” knowledge in a CoP, offering a more secure environment will contribute to sharing, the overall effectiveness of the community, and in reality contribution to the bottom line (even in a non-profit organization).

What is challenging when it comes to security in a CoP is the scope or reach of the community. A CoP can be internal to an organization, can include external partners, and can be open to a variety of public members. The “practitioners” involved in a community of practice and the nature of the shared data will greatly influence the level of security that is needed in a CoP.

Virtual Communities of Practice

Traditional communities are place-based and have membership according to norms. The community usually clearly defines who is a member and who is not. In contrast, virtual communities exist according to identification to an idea or task, rather than place. V-CoPs are

organized around an activity, and they are formed as a need arises (Squires and Johnson, 2000). Virtual communities do not need formal boundaries for they can be fluid. Norms do not dominate in V-CoPs, in contrast to more traditional CoPs, which allows for greater individual control. In a V-CoP, the Internet becomes the place for the community. V-CoPs have increased the parameters of what is known as a community (Palloff and Pratt, 1999). Both virtual communities and CoPs have life cycles. Palloff and Pratt (1999) outline five stages of the life cycle of community development: forming, norming, storming, performing, and adjourning. Thus, in CoPs and V-CoPs “language, practices, customs, and resources develop over time” (Squire and Johnson, 2000).

The definition of a V-CoP is similar to a traditional CoP, the primary difference being that a V-CoP is a group separated by space and time that uses networked technologies in one form or another to collaborate and communicate. The members of the V-CoP will almost certainly use the community’s artifacts (technology, processes, symbols, pictures, policies, etc.) (Johnson, 2001). V-CoPs can consist of a larger, loosely knit group of individuals engaged in a shared practice who may not expect to meet face-to-face and who may not know each other (Wasko and Faraj, 2005). Even though members may not ever meet face-to-face, they are able to share a great deal of knowledge. Like CoPs, V-CoPs can be self organizing groups and open activity systems focused on a shared practice. V-CoPs may be predetermined and by-invitation-only groups. Some of these groups exist as both open activity systems and by-invitation-only systems, a common trait in systems where certain types of information are made available to the public at large, and core or invited members must use a password, or be part of an access

control list (ACL) that permits their access to restricted data that is deemed more sensitive than public access data (Anderson, 1996).

V-CoPs, like any other network environment, must adhere to the same rules as a traditional network infrastructure found in any business environment. The policies and procedures implemented must follow standard and well formed practices (SANS.org, 2005). However, like any other virtual environment, proper education and training must be done to ensure that users do not compromise sensitive data, nor unwillingly disclose information or knowledge that would negatively impact their organization or their personal lives.

Deterrence Theory

There are two forms of deterrence theory, classical and contemporary (Higgins, 2005). The classical form assumes that individuals are rational beings and, therefore, think and act in a rational manner. Also, they perform behaviors they perceive as pleasurable or beneficial and avoid behaviors they perceive as painful or costly in either financial or physical terms. Key to this theory is an individual's belief that illicit behavior will be detected, will be harshly punished, and will be quickly resolved. Therefore, when the threat of punishment is perceived by the potential perpetrator to be certain, severe, and swift, the perceived cost of an illicit behavior increases, triggering caution in the individual who could refrain from the behavior, thereby deterring and reducing the illicit behavior. By demonstrating that certainty rather than severity was the most important deterrent measure, the research suggests that classical deterrence

theory is not a complete enough model to understand what deters individuals from crime (Higgins, 2005). If an organization has put in place proper levels of deterrents and has properly educated its employees, there will be a reduced likelihood of breach by external hackers. Deterrence theory can be of further use when the users of a system, like a V-CoP, are educated on the potential costs associated with breaches in secure data. There should be a heightened sensitivity to security policy measures and practices.

Contemporary deterrence theory recognizes the various problems with classical deterrence theory, such as assuming that people are rational beings who avoid performing acts that have a high negative cost. However, research has shown that people are more likely to avoid performing illicit acts, such as computer hacking, if there is a high probability of being caught instead of on the actual punishment for the act (Higgins, 2005). Contemporary deterrence theory enhances the classical theory through the addition of other measures that represent inhibitions and motivations for illicit acts (Higgins, 2005). For example, Grasmick and Bursik (1990) suggest that including conscience measures, such as shame and guilt, contributes to the understanding of how to deter people from illicit behavior. Grasmick and Bursik (1990) more specifically suggest that “an understanding of the level of self-disapproval would demonstrate inhibitory effects on illicit behavior, because of the self-stigmatizing implications they provide”.

With the rising incidents of computer abuse, organizations are searching for better methods of deterrence. Based on the general application of deterrence theory, organizations can reduce computer abuse by implementing standard security policy measures such as anti-

virus systems, password protection schemes, rigorous enforcement of computer security policies, and fostering security awareness in employees through special security education (Lee, 2003).

Classical deterrence theory explains how security measures implemented by organizations rely primarily on the technology used to protect information systems without considering other factors, such as people issues and processes that are in place that may be a security weakness. In particular, Eloff and von Solms (2000) provide a hierarchical framework for security management. Their framework includes two major elements: technology and processes. However, they do not include another piece of the security puzzle, the human aspect (Lee, 2003). A recent joint study by CSI and the FBI documents that the most serious losses in companies are committed by unauthorized insider access (Richardson, 2008). Dhillon and Backhouse (2001) pointed out that information security is a social and organizational issue because people use the system. Thus, it is the humans interacting with, and responsible for systems that have the biggest impact on the security of individual systems and the organization or V-CoP.

Deterrence theory can be applied to information security in a number of ways. Breaches can occur from inside or outside an organization. Usually, insider breaches arise from legitimate users violating a standard computer security policy. However, malicious breaches may be perpetrated from within the organization but also, and more often, from outside the organization. If the focus is on the computer attacker, which will be referred to as a malicious hacker, then deterrence theory can be used to create an environment where the malicious

hacker risks such severe penalties that considering hacking the system is not worth the potential risks of being caught. Also, if the malicious hacker perceives that there is a high probability of being discovered and caught, there is a higher likelihood that the malicious hacker will avoid the risk of detection for more target rich environments. If the focus is on the legitimate user of the system, for example, a member of a V-CoP, then properly educating the user on the potential outcomes of not strictly following security policies and procedures may help to motivate the user to follow the policies and procedures.

Information Security (InfoSec)

Computer security or information security (InfoSec) is becoming a more complex issue as organizations store a vast array of data that can range from general sales data to top secret military information. Further complicated by virtual environments and the communication that takes place over the ether, computer security has become a key subject of interest within organizations. Changes in the way organizations share and store data provides for an environment where opportunistic hackers can take advantage of data repositories that are available online and data transmission between remote sites by virtual members of online communities such as V-CoPs. The AICPA (American Institute of Certified Public Accountants) clearly identified InfoSec controls as the number one issue of the top ten technology issues (Cryton and Tie, 2001). Also, information security is a business issue and not a technical issue (Von Solms and Von Solms, 2004). Lastly, information security governance is a multi-

dimensional discipline. Information security governance is a complex issue, there is no silver bullet or single 'off the shelf' solution (von Solms and von Solms, 2004).

InfoSec is concerned with confidentiality, integrity, and availability. Confidentiality has been the primary focus, but Clark and Wilson argue that the integrity of information is more important than its confidentiality. Integrity is defined as "information is not modified in unauthorized ways, that it is internally consistent and consistent with the real-world objects that it represents, and that the system performs correctly" (Blake, 2000). The Clark-Wilson model includes two important principles of integrity. The principle of separation of duty specifies that no single person should perform a task from beginning to end. Any task should be performed by at least two people to avoid fraud by one person acting alone. The principle of well-formed transaction is defined as a transaction where the user is unable to manipulate data arbitrarily, but only in constrained ways that preserve or ensure the integrity of the data. The three goals of integrity are to prevent unauthorized modifications, to maintain internal and external consistency, and to prevent authorized but improper modifications. The Clark-Wilson Model divides data into two categories – constrained and unconstrained data items. Constrained data items (CDI) are data items for which the integrity model is applied and unconstrained data items (UDI) are not covered by the model (Blake, 2000). It is useful in constructing a V-CoP security policy to know which type of shared data would be considered CDI and which would be UDI. Knowing the necessity of data integrity is an important part of a virtual community.

Another model, the Bell-Lapuda model, focuses on data confidentiality and access to data that is classified. The entities in this model are divided into subjects and objects within the information system. A secure state or ideal state is defined and proven, and then each state transition preserves security by moving from secure state to secure state. Throughout a virtual communication exchange, as found in V-CoPs, the model is built on the concept of a state machine with a set of allowable states or positions that enable the secure execution of data sharing. The transition from one state to another state is defined by transition functions. A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object to determine if the subject is authorized for the specific access model (Bell, 2005). Ultimately, what the model strives to achieve is a consistent determination of security based on a set of prescribed rules and procedures. In a V-CoP, what is important is the assurance of how data is shared, and how users interact with each other in a secure environment, not violating the security policies of their organization.

When examining security models in the context of virtual communications and virtual data repositories, as found in a V-CoP, computer security should be addressed first and foremost from the user perspective. The end-user is usually an operations employee that uses the system for daily work, but could also refer to senior executives, as they have the responsibility for ensuring that proper data security measures are implemented and that the personnel responsible for managing data security have adequate preparation and training

(SANS.ORG, 2005). It is true that end-users make mistakes on a regular basis that can lead to security breaches and they are a major cause of security problems within an organization. End-users are unintentionally contributing to the success of computer hackers by failing to follow routine basic computer security policies (SANS.ORG, 2005; Hakala, 2008). End-users ignorance can be tragic in a virtual environment where users may be located anywhere across the world and the security safeguards in place may vary from place to place.

Human error is the major cause of most computer breaches, including such simple errors as the improper securing of laptops, backup tapes, and disks (Baker, 2008; Hakala, 2008; McGlasson, 2008; Whitman, 2004). One specific example involves a laptop that was stolen from an NIH researcher containing the unencrypted details of over 2,500 patients involved in a clinical trial (Greenemeier, 2008). In a V-CoP, data is often downloaded and stored on portable devices so proper security of these devices is critical. It is plain to see that proper security procedures need to be followed to avert such potential calamities. What is unfortunate is that information management systems are traditionally developed without any security considerations, for example, because the users of the systems know each other, share the same goal, and share a fixed set of administrative rules which is not necessarily true in today's environment (Boella and van der Torre, 2006).

Security issues are common because users fail to perform basic information security policy tasks such as installing and keeping up to date anti-virus software on their systems (SANS.org, 2005). End-users make the mistake of opening email attachments without properly checking the source and content of the file. If the end-users back up their files, they neglect to

test the backup to make sure that the backup was successfully made. Lastly, they may be connected to a wireless network and still connect to the network or Internet using a modem, which can result in numerous security issues because the end-user may be inadvertently circumventing the system security features that are in place (SANS.ORG, 2005). These issues can severely affect the operations of a V-CoP by unknowingly spreading computer viruses, Trojans, or other InfoSec threats.

There is a need for greater levels of awareness, education, and security policy information within organizations (Whitman, 2004). Even though many companies have a security policy in place, there are inconsistencies and users are not regularly trained or tested on security risks and threats. There is also confusion over who controls the data that is stored in the information systems of the organization (Yampolskiy, and Govindaraju, 2007) which would include access to shared data in a V-CoP since the data may be stored on the same servers. Key to this research is not only the education of users to the potential disasters that can occur through every day events such as making sure they keep their password secret, logging off or locking their computers when leaving their office space, backing up important data files, etc., but also, how to avoid security breaches at all. Even with today's security improvements, the hackers are staying one step ahead of the security system manufacturers.

V-CoP end-user security issues help to support the notion of properly educating these same end-users on the issues involved in lack of adherence to the organization's security policy. If end-users are properly educated on the risks and potential damage that can be done by hackers, they will be more likely to follow the organization's security policy. Deterrence

education has been found to be effective in keeping outsiders and insiders from attempting to hack or misuse a system. Hoffer and Straub (1990) found that deterrents have been effective in lowering computer abuse. However, proper reporting of incidences must also be part of the security process. In fact, another study found that computer abusers were often discovered by accident, through normal system controls and purposeful detection. But, only 9% of abuses were reported to outside agencies (partly due to ignorance). More specifically, 90% of respondents feared negative publicity if they reported; 75% felt that competition would use this information against them; and 54% of respondents did not know they could report the incidences (Richardson, 2003). So not only do organizations need to provide education to end-users and proper deterrents to prevent computer abuse, but also a clear policy on reporting abuses.

Points and Causes of Security Breaches

Unfortunately, there are many causes that lead to security breaches within a system, with human error being the key aspect. In the 2003 CSI/FBI survey, respondents cited their Internet connection as a frequent point of attack, up from 74% in 2002 to 78% in 2003 (Whitman, 2004). Furthermore, the CSI/FBI survey revealed the following threats to information security:

- Act of human error or failure (e.g. accidents or employee mistakes).*
- Compromises to intellectual property (e.g. piracy, copyright infringement).*
- Deliberate acts of espionage or trespass (e.g. unauthorized access and/or data collection).*

- Deliberate acts of information extortion (e.g. blackmail of information disclosure).
- Deliberate acts of sabotage or vandalism (e.g. destruction of systems or information).
- Deliberate software attacks (e.g. viruses, worms, macros, denial of service).*
- Quality of service deviations from service providers.
- Technical hardware failures or errors (e.g. equipment failure)
- Technical software failures or errors (bugs, code problems, unknown loopholes).*
- Technological obsolescence (antiquated or outdated technologies).*

*More closely relates to V-CoP

Almost all of these threats would apply to a V-CoP. Accidents made by employees of the system could impact the V-CoP by not properly virus checking a document before uploading it to the system or by placing confidential data in an open forum where anyone can view the data. One example is when Kaiser Permanente accidentally posted patient medical records and test results on a public area of a corporate site several years ago (Rosencrance, 2005). Compromises to intellectual property are always a risk through plagiarism and misquoting of source data posted to a V-CoP. It is important that the members of the V-CoP can fully trust the information that is permanently posted to the V-CoP site.

The top security threat for over 8 years is virus attacks and the fourth ranked threat was DOS (denial of service), which are deliberate software attacks (Whitman, 2004). These can be particularly hazardous to a V-CoP as a software virus innocuously embedded into a shared file

could easily be replicated to all of the systems of the members of the V-CoP. Employee mistakes and failures to follow policy represent a dominant threat requiring the implementation of controls to reduce the frequency and severity of such attacks. Respondents to the CSI/FBI survey stated that they spent the most money on human mistakes, technical problems, and service-provider problems (Richardson, 2008). Virus incidents occurred most frequently in about 50% of the respondents' organizations. Next, insider abuse was around 44% followed by physical theft (e.g. laptops, etc.) at 42%. Even in the medical community, 11% of general practitioners in Great Britain experienced computer theft (Anderson, 1996). About 1 in 10 reported a domain name system (DNS) incident, which was up 2% from the previous year. Over 25% reported being victims of a "targeted attack", meaning an attack aimed specifically at their organization from an outside hacker. Of reporting organizations, 68% said they had or were developing a formal information security policy, with only 1% stating that they did not have a policy (Richardson, 2008).

The 2008 Data Breach Investigations Report (Baker, et.al., 2008) discovered that more than half of the over 500 data breaches researched required little or no skill to perpetrate. The computer hackers utilized tools easily downloadable from the internet to commit their illicit acts. Basic run-of-the-mill tools and precautions would have prevented these hacks from occurring (Richardson, 2008). Furthermore, Richardson found that the four categories of highest incidence are viruses, insider abuse, laptop theft, and unauthorized access to systems. In the medical world, software bugs could alter the numbers in a laboratory report without changing it so grossly that it would be rejected, and viruses have already destroyed clinical

information (Anderson, 1996). Concern has also been expressed that the lack of standards in clinical EDI (electronic data interchange) may lead to data being interpreted incorrectly or differently by different systems, with potentially life-threatening effect (Anderson, 1996).

Most breaches resulted from a combination of events rather than a single action (Baker, 2008). He found that 90% of known vulnerabilities exploited by these attacks had patches available for at least 6 months prior to the breach. Investigators concluded that nearly all breaches would likely have been prevented if basic security controls had been in place at the time of the attack. Members of a V-CoP are likely targets since they primarily use virtual communications that often take place over network connections that utilize the public network. What makes most security breaches complex is that they resulted from multiple intra-category events, meaning the hackers had utilized several types of techniques and/or tools and many encompassed several threat categories (Baker, 2008). Security breaches are a particularly dangerous situation in online communities as hackers with little or no skill can launch sophisticated attacks against sites and systems with readily available free software. Software such as LophtCrack, a brute force password attack tool, and VisualRoute, a legitimate tool that reveals information about a site such as the registrant of the domain name, IP address, range, and more, are routinely used to hack or gather information about a site so that it can be hacked. Members of V-CoPs must be aware of the ease of attack and adjust their online behavior to reflect a higher level of caution and awareness.

Hacking leads to more data breaches than any other category by a margin of two to one. The types of hacking are broken down as follows: application/service layer = 39%, OS/platform

layer = 23%, exploits known vulnerability = 18%, use of back door = 15%, exploits unknown vulnerability = 5%. A patch deployment strategy focusing on coverage and consistency is far more effective at preventing data breaches than fire drills attempting to patch particular systems as soon as patches are released (Baker, 2008). Results suggest that management needs to (1) become more informed of the potential for security breaches, (2) increase their awareness in key areas, and (3) recognize that their overall level of concern for security may underestimate the potential risk inherent in the highly connected environment in which they operate” (Loch et al.,1992). Application of these procedures is key not only to the organization as a whole, but to the V-CoPs that are operating throughout an organization and their partners.

Hackers Geographic Location and International Issues

An increasing number of hackers are becoming organized around the world, making it more difficult for law enforcement to prosecute these hackers and bring them to justice (McGlasson, 2008). In the case of TJX (parent company of the TJ Maxx chain of retail stores), only 3 of the 11 defendants lived in the United States (McGlasson, 2008). With the advent of the connected world through the internet and specifically the World Wide Web, a computer hacker can live anywhere in the world and launch attacks with relative anonymity and with almost no cost.

Computer ethics studies have found that individuals from differing origins had somewhat different perspectives with regard to computer ethics (Whitman et al., 1999). It is important to use caution when placing expectations on individuals from other cultures

regarding their ethical performance. Managers must attempt to understand their perspectives and educate them on the organization's perspectives (Whitman, M. 2004).

Cost of Security Breaches

A study by Forrester Research has estimated that an average security breach can cost a company between \$90 and \$305 per record. Included in the costs are legal fees, call center time, lost productivity, regulatory fines, stock price loss, and customer losses (Gaudin, 2007). Even so, it is difficult to put a price tag on a security breach, and according to the survey, as many as 25% of the companies did not know, or do not know, how to put a price on the cost of a breach. Some losses can be so significant that it can put a company out of business. Kark found that discovery, response, and notification costs were averaged out to be about \$50 per lost record. The cost of record loss has increased primarily due to lost employee productivity and increased public attention.

The 2008 CSI Computer Crime and Security Survey found that the most expensive security breaches were for financial fraud, with an annual average loss estimated at almost \$500,000 per incident. Next were "bot" computers (computers unknowingly running software programs that can cause or are causing security holes) within the organization's network with a loss estimate of almost \$350,000 per incident (Richardson, 2008). The average loss per respondent was \$288,618, down from \$345,005 in the previous year, but up from the low of \$167,713. Financial fraud costs the most at an average of \$463,100 per incident, followed by bot computers reported to cost \$345,600. Loss of customer and employee confidential data

averaged \$241,000 and \$268,000, respectively. Virus costs were down and cost on average only \$40,141 per incident – which is somewhat encouraging since this is the most common type of security breach (Richardson, 2008). Even though virus costs were down per incident, in 2002 the worldwide cost of worms and viruses was estimated at \$45 billion and in 2003 the costs had risen to \$45 billion by August (Kjaerland, 2006). Viruses lead to other breaches and are easily replicable across networks. The vast quantities of virus infections have led to this extremely large dollar cost and there is little sign of a significant decrease in sight (Kjaerland, 2006).

Security Awareness and Training

Organizations need to increase employee training and awareness to avoid accidental and careless mistakes. According to Hoffer and Straub (1989), deterrence is most effective when the subject has a realistic expectation of apprehension, a fear of the sanctions, and reasonable expectation that the sanctions will be applied. Organizations must, however, be aware of the toll that excessive preventative measures can play on the performance of a system and/or application (Whitman, 2004).

Feedback from 522 computer security professionals found that 53 percent of the respondents said that their organizations allocated 5 percent or less of their overall IT budget to information security, and 42 percent spend less than 1 percent of their security dollars on awareness programs (Richardson, 2008). Spending only 1 percent is an alarmingly low expenditure rate when one considers the cost of dealing with security breaches and is a problem that can either mean that companies are not taking awareness seriously or they do

not think that it is worth the effort. In the same survey, companies were asked about the measures that they use to gauge the effectiveness of their security awareness programs. Only 18% of companies do not use awareness training at all, which is good news. About 4 of 5 organizations do some type of awareness training regarding security risks and appropriate handling of sensitive data. However, 32% make no effort to measure the effect of this training on their organization (Richardson, 2008). Furthermore, there was no mention of the frequency of the training and whether employees were randomly tested to see if they had retained what they had been taught.

Another concern in the survey was that organizations are becoming somewhat less actively involved in sharing. The number of respondents who are not members of an information sharing organization has grown over the past two years. For example, membership in InfraGard dropped by 6 percent. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. ISAC (Information Sharing and Analysis Center) groups also saw a dip in membership (Richardson, 2008). There is no clear surge in growth of membership in such groups. As in previous years, only about 25% of respondents say they have contacted a law enforcement agency about security breaches.

Not realizing the core importance of information security awareness among users will lead to security issues in many organizations because no proper awareness programs exist. Also, users are unaware of the risks of using the company's IT infrastructure, and the potential damage that the users can cause. Users that are properly made aware of the risks and

potential damage that can take place are more likely to take security more seriously. Furthermore they are often not even aware of the information security policies, procedures, and standards existing in the organization. Users cannot be held responsible for security problems if they are not told what such security problems are and what they should do to prevent them (Von Solms and Von Solms, 2004).

Ways to Avoid Data Compromises (Breaches)

There are many ways to avoid breaches or computer security incidences. McGlasson found that it was important that third party handlers of data is as secure as the company that is providing the actual data, and that it is critical to make sure that data is appropriately encrypted when it leaves the organization (McGlasson, 2008). It is also important to make sure that systems are compliant with any local and federal regulations and laws, and if the organization is hacked, to promptly notify partners and law enforcement agencies of the attack. Areas of protection must exist at both the local and global levels (Cuppens, 2005). The local level would include threats to information located on a single system. At this level, regular audits and backups are necessary to maintain data integrity. At the global level, it is necessary to create a security policy to control global threats to the confidentiality, integrity, or availability of the data which arise from ill-considered aggregation of systems and other causes (Anderson, 1996).

Specifically, systems administrators and managers need to begin with an understanding of the threats that their systems face, and then they must study the vulnerabilities that are

inherent to the identified threats. Mitigation efforts should be focused in a number of areas, starting with the users and their awareness of what they should do to protect the information resources of the organization. Next, it is important to ensure that essential controls are met. Following through on security policies so that they are actually implemented and ensuring that a basic set of controls is consistently met across the organization is also necessary.

Organizations must find, track, and assess data. They need to know where data is located and the category of data (i.e., not sensitive, sensitive, secret, etc.). Based on the hundreds of breaches investigated, efforts to locate, catalogue, track, and address the risks of data stored in and flowing through information assets are highly beneficial in reducing the likelihood of data compromise (Baker, 2008). Organizations should strategically identify what systems should be monitored and what events are alertable (Baker, 2008). Steps should then be taken to ensure alerts are noticed and acted upon when they do happen.

The goal of an organization should be to implement security measures so that it costs the illicit hacker more to compromise the system than other available targets. Softer or easier targets are still in ample supply. In 82% of cases, victims possessed the ability to discover the breach had they been more diligent in monitoring and analyzing event-related information available to them at the time of the incident. In V-CoPs, members must be alert and carefully assuring that confidential and proprietary data and information is not carelessly posted or sent to insecure and unknown sources. Overall, the breakdown is in the process. Organizations seem to lack a fully proceduralized routine for collecting, analyzing, and reporting on log activity outside of the norm (Baker, 2008). Furthermore, 87% of breaches could have been avoided if

reasonable security controls had been in place at the time of the incident (Baker, 2008). The following recommendations provide a starting point (Baker, 2008):

- Align process with policy – 59% of victims knew what to do, and intended to do it, but did not follow through. Controls focused on accountability and ensuring that policies are carried out can be extremely effective in mitigating the risk of data compromise.
- Achieve essential then worry about excellent – 83% of breaches were caused by attacks not considered to be highly difficult and 85% were opportunistic. Hackers prefer to exploit weaknesses rather than strengths (if they do not find an easy target at a particular organization, they will move on to easier targets). A V-CoP that is unsecure will be an easy target for hackers. Organizations need to identify a set of essential controls and ensure their implementation across the organization and then move on to more advanced controls.
- Create a data retention plan – 66% of breaches involved data that the victim did not know was on the system. Organizations should identify and quantify the types of data retained during business activities and then work to categorize data based on risk and liability (i.e., what data cannot suffer compromise and prioritize accordingly). V-CoPs must make sure that the data shared and stored in the data repository is deleted when no longer needed or used, especially when this data is confidential in nature. Backups of data must also occur within the V-CoP so that if an attack or system malfunction occurs the data can be readily and easily restored to a correct state.
- Monitor event logs – evidence of events leading up to 82% of data breaches was available to the organization prior to actual compromise, but information regarding the attack was neither noticed nor acted upon. The end-user is not going to be held responsible for reading the logs since they should not have access, but a procedure must be in place for a V-CoP where the log data is part of the normal review process of the organization.
- Create an incident response plan – the victim organization must be ready to respond. When a member of a V-CoP detects or suspects an incident they must know the proper procedure for reporting the incident.
- Increase awareness – implementing a required awareness program is the key focus of the proposal to increase awareness through education and training. Users that

are made aware of the potential threats to a system and the ramifications of these threats should be better stewards of their V-CoPs realms.

- Engage in mock incident testing - organizations should undergo routine training in the area of incident response. Attendance should be required as mandatory by policy and is key to the proposal to test if the member of a V-CoP has increased their awareness and ability to properly respond to security threats and attacks.

There are three basic controls for implementing security in any environment – from internal systems to external virtual environment systems (Lampson, 2004):

- Authenticating principals – determines who made a request (person, program, or group). In a virtual environment this is particularly difficult since authentication is based on the assumption that the person on the other end of the communication is who they claim to be based on their electronic credentials.
- Authorizing access – determines who is trusted to do what to an object (read, write, copy, delete, etc.). V-CoPs must have a clear policy that monitors and specifies access control based on need and requirement. The rule of thumb is to grant the member (end-user) the minimum rights needed to effectively participate in the community.
- Auditing the guard's decisions – used to determine what happened and why did the guard let a certain principal perform a task on an object. Follow up on access and why certain members were permitted access to certain data (objects) on the practice site. Ownership and control plays an important role. The owner of the data should be responsible for controlling who has access to the data, can modify the content, can delete the file, and can change permissions.

It is important that knowledge providers should not give up their autonomy to prohibit access to users they do not trust, even when they satisfy the security rules of the virtual community. The policy rules for managing knowledge in a secure way concern not only which knowledge the users are prohibited or permitted to access, but also which regulations the community members are allowed or obliged to enforce (Boella and van der Torre, 2006).

Threats to Confidentiality

According to Anderson (1996), threats were common from insider abuse and were compounded by the aggregation of data within organizations. As more and more organizations collect and store more data, there are more targets available to would-be hackers or opportunists who would take advantage of inadequately secured data repositories, especially in a V-CoP. Self-organizing systems can be more difficult to protect as the membership can be varied and constantly changing. The more valuable the data, the higher the likelihood of compromise as worthless data does not need to be as closely guarded. The fragmentation of much of the data within an organization leads to other issues as this data is most likely not properly protected. In the medical world, for example, a banker had access to his clients' medical records and called in loans of those with health issues. Abuses, misuse, or mishandling of information is common in most fields. The real political struggle is over control, such as who controls the data and the data's flow within the organization.

Someone must be held responsible for every piece of data collected and stored within an organization's network. Determining how ownership is to be managed is a key aspect of the security policy as ultimately the owner will be held responsible for the protection of this data (or at least needs to be aware of where it is stored and who has access).

Providing Access

Access control lists (ACL) are lists of what users and programs can access the system or data, and what type of access they have. One way to look at access in the context of the

security policy is that records, depending upon their level of security, will be marked with an ACL and people or processes that are not on the list will be denied access to the information in any form (Anderson, 1996). These lists must be consistent across all systems in the organization so that holes are not created by competing lists or inheritance from a global to a local list. Access can range from none, to read only, to modify, to create and delete. As with ownership of the actual data, someone or some department must be responsible for maintaining who has the ability to change or modify the ACL for the specified data. In a highly confidential environment, access may not be granted to the IT administrator if he should not have access to view or change the data (Anderson, 1996). Strong notification requirements are needed to help control fraud and other misuses of data, particularly highly sensitive and valuable data (Anderson, 1996).

Another consideration that organizations need to be aware of is persistence or the length of time that data must be kept. As mentioned earlier, a well-defined retention policy must be created and enforced for systems and virtual communities. There are local, state, and federal laws on the length of time that specific types of data must be kept by various organizations and businesses (such as banks, hospitals, etc.). Information that is currently in the system should be updated through appending new data rather than deleting recent versions, and data should only be deleted for records that have expired or are found to be corrupt (Merali and Davies, 2001). A record should also be kept of who accessed information and what they did to that information. Did they just view the information or did they append or modify the information? A change log must be kept to ensure proper attribution of access.

Information Security Policies

An InfoSec policy contains rules and regulations that are laid out in written form that clearly defines how an organization is going to protect its valuable information resources. InfoSec policies include acceptable use of computer systems and data, rules and regulations for accessing data, and other topics related to confidentiality, integrity, and availability of information resources. According to Bishop, "A security policy, a specific statement of what is and is not allowed, defines the system's security. If the system always stays in states that are allowed, and users can only perform actions that are allowed, the system is secure. If the system can enter a disallowed state, or if a user can successfully execute a disallowed action, the system is non-secure" (Bishop, 2003). In a V-CoP the security policy must be as vigorously enforced as in any other environment. The key issue is when members are from organizations with different policies, so the members or creators of the V-CoP must come up with a common or global policy that all members can agree upon. Creating the global policy may be as simple as finding the common elements from all of the member organizations' policies and enforcing these common rules and regulations.

The SANS Institute defines a security policy as "a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities" (SANS.ORG, 2008). The primary purpose of the security policy is to regulate access to data,

maintain proper controls over the information that is stored on an organization's computer system, and to mandate the proper use of the computer resources available to the user (Anderson, 1996; Bishop, 2003; Cuppens, 2006). Lastly, according to Cholvy and Belin, "the primary goal of a security policy is to specify [the] means for facing a given environment of threats" or as a specific case of regulation (Cholvy and Belin, 1997).

Without an information security policy, there would be no apparent requirement for secure practices, and security would be either ignored or implemented in an ad hoc manner, and thus, control could be either too rigid or completely missing (Boella, and van der Torre, 2006). An information security plan must be based on identified risks. It is therefore essential that a company must base its information security plan on some type of risk analysis exercise (Cuppens, 1996; Von Solms, and Von Solms, 2004).

Security policies in a distributed environment provide a greater challenge, particularly when the policy applies to multiple organizations or organizations and groups from other companies. Controlling the quality of information that is shared within a V-CoP is critical to its success (Neus, 2001). Key to a security policy: is the control of data: who is responsible and who ultimately owns the data. There is local knowledge and global knowledge. The local knowledge should be handled and controlled by the local department or organization that is part of the V-CoP. The global knowledge is that knowledge which is available to all members of the community and is distinguished from knowledge that is in the public domain. In this model of local and global control, information or document providers retain the control of their documents and they specify in local policies the conditions of use of their documents which

means that they can determine what types of access are permitted to various documents per user or per group. If information owners are not clearly defined and held responsible for the security of the information under their control, severe risks do arise. Accountability for information security must be shared by all employees, and not only the information security manager (von Solms and von Solms, 2004).

The knowledge providers prefer not to give up their own power to enforce local policies for the access to the documents they control. There are cases where security administrators are not fully trustworthy, for example, when multinational virtual communities are headed by foreign countries with varying security standards (Boella and van der Torre, 2006). So, leaving autonomy to the knowledge providers must be balanced with the requirement that their local access policies should be organized according to a global policy defining how the knowledge should be shared among participants. As van Elst et al. (2004) observe organizations, departments, groups and individual experts develop their particular views on a given subject. In V-CoPs, global access controls cannot be directly implemented, since no one owns all of the documents or information in the system. Global policies are issued and enforced by a *community authorization service (CAS)*: A given group or community runs a CAS server to track its membership and contains fine-grained access-control policies. A user wishing to access community resources contacts the CAS server, which delegates rights to the user based on the request and the user's role (i.e., what access they have to which documents or other information) within the community. A key problem associated with the formation and

operation of distributed virtual communities is that of how to specify and enforce these community policies (Pearlman et al., 2002).

One example of this global and local policy hierarchy is the interconnection of electronic health record (EHR) systems (Gritzalis and Lambrinoudakis, 2004). EHR systems facilitate the collaboration of independent health care units (HCU), with each unit remaining sovereign in its own domain and defining its own security policy (similar to a local security policy). However, users in one domain may ask to access information in any other domain (i.e., global policy). The network of interconnected sites is not static. A new HCU may join the network at any time. There is no central authority administrating or even enforcing a common policy to all interconnected sites. The fact that medical information can be accessed from some unknown remote location, possibly belonging to a different domain and thus exhibiting a different security policy, imposes the need to treat the data in accordance to specific security attributes (policies) attached to it. No predefined trust relations among individual HCUs or groups of units can be assumed. Trust evaluations should be dynamic. The security requirements that have been identified include: Each HCU should have the freedom to design its own security policy and to enforce it within its domain. Through the interconnection of different domains, a multiple-security-policies environment will emerge. Consequently, several policy conflicts may occur, posing the need for a 'resolving' mechanism. Static and rigid security policies, based on the currently dominant "subject—to—object" paradigm are not suitable. The requirement is for policies that are context-aware and adaptable. The integrity and confidentiality of medical information should be ensured. Medical records, when communicated to remote health care

units (different domains) should be protected through their own access control policy. Users should be authenticated in their local EHR systems (local domain). When they request authorization to access resources in some remote system they should not be asked to re-submit their credentials or to provide any additional credentials (Gritzalis and Lambrinoudakis, 2004).

At the global level, users should adhere to an agreed upon or standard policy that can be applied to all users of the V-CoP (or community) and that do not violate the local policies implemented by the local owners of the system. An agreed upon policy for the community needs to be defined that does not violate the local policies from each member's organization from the V-CoP. For example, at the global level, participants should not communicate their passwords or distribute copyrighted files by means of the community. If they violate these basic global policies, they are banned from the community, since the membership to the system is under the control of the global authority. There are policies that apply to other policies, such as global policies that constrain or permit local policies (Sloman, 1994). The global authority could oblige local ones to forbid access, permit-to-permit access, or permit-to-forbid access. However, it is not sufficient that the global obligation to permit or oblige access is satisfied by the fact that the local provider issues permission or an obligation. Norms are ineffective if they are not enforced by the system who issued them: violations of norms should be recognized as such and sanctioned according to the standards set in the policy (Boella and van der Torre, 2006).

Configuring the network security policies globally and locally remains a "complex and error-prone task due to rule dependency semantics and the interaction between policies in the

network” (Hamed and Al-Shaer, 2006), but will depend upon the type of V-CoP. Security policy complexity is likely to increase as the size of the network increases. A successful deployment of a network security system requires global analysis of policy configurations of all network security devices in order to avoid policy conflicts and inconsistency. Increasing threats of network attacks against security devices requires careful configuration. Firewalls and IPSec (internet protocol security) gateways have become important integrated elements not only in enterprise networks but also in small and home networks. Deploying these tools provides for incredible flexibility for customizing the proper protection for different networks and applications. But, even expert administrators can make serious mistakes when configuring the security policy of these devices. Administrators must be aware of policy conflict types and the lack of automated verification of security policies (Hamed and Al-Shaer, 2006). In a V-CoP, policy configuration is particularly problematic where there is likely to be both local and global policy rules. If these rules conflict or overlap, they may open a hole in the security of the community and provide easy access to sensitive documents and other non-public information. A V-CoP policy would include many of the same policies found in a traditional security policy. However, when multiple organizations are represented by the V-CoP the primary members must agree upon what global policies are to be followed by all members of the community and which policies may be specific to an organization. These policy conflicts occur due to rule misconfiguration within a single policy or between policies in different devices (Hamed and Al-Shaer, 2006). ACLs control who has access, what they have access to, and what level or type of access they have to the information.

When conflicts occur, they usually exist between rules in the same security device (intrapolicy conflicts) or in different devices (interpolicy conflicts). Intrapolicy conflicts occur when different rule orderings may imply different and incorrect policy semantics. Some rules may be concealed by other rules, resulting in an incorrect policy. Interpolicy conflicts could exist between policies of different devices. For example, a firewall might block traffic that is permitted by another downstream firewall, or an upstream IPSec device might protect traffic that is not protected by the peer downstream device (Hamed and Al-Shaer, 2006). Once again, human error is the critical factor in these security policy conflicts and can lead to severe consequences if not properly managed.

Simulation and Training in Computer Security

Simulation and training have long been used to train people for a wide variety of tasks. The most well known is the flight simulator whose origins go back to 1910 when the Sanders Teacher was introduced (Rolfe and Staples, 1988). Since that time, simulation has grown in scope and is being used in almost every field from medicine to traffic control.

Medicine has seen tremendous advances through the use of simulation. A major benefit is that doctors can practice procedures and diagnostics in a simulated environment without any human cost (Friedrich, 2002). For example, educators at Penn State University have created a program for anesthesia residents called “The First Three Days of Anesthesia” where they are introduced to the various tasks involved in delivering anesthesia to a patient.

At the end of the three days, they are then given the opportunity to deliver anesthesia to a simulator (Friedrich, 2002). Errors in a simulated environment do not result in human trauma or fatalities, nor do they result in financial loss due to user error.

Simulation is also used in education and to train students on such things as business, information technology, chemistry, biology, physics, math, and even the social sciences. Many colleges and universities offer virtual labs to their students to perform experiments, run tests, check solutions, and more.

Simulation has also been utilized in computer security. One example is the Center for the Information Systems Studies and Research (CISR) at the Naval Postgraduate School where a broad program in computer security education has been established (Irvine, 2004). Part of this effort has been the creation of CyberCIEGE, a computer simulation game that teaches computer security principles. Players of the game construct computer networks and make choices impacting the game's virtual users' ability to protect valuable assets. The game includes a language that enables the user to express different security scenarios and a variety of different security policies (Irvine, 2004). The CyberCIEGE tool can be used to train security administrators on simple tasks such as password length, opening emails with unknown attachments, identification of other users, and more.

Another computer security training tool called RINSE (Real-Time Immersive Network Simulation Environment) is a simulator being built to support large-scale network security preparedness and training exercises (Liljenstam et. al., 2006). The goal of RINSE is to create a realistic environment where the simulated network behaves as if a real attack were taking

place. The system will support hundreds of players and a modeled network composed of hundreds of local area networks (LANs). Players will diagnose events and try to counter the attacks through the RINSE interface.

Taxonomy of Computer Security Incidents

Computer security incidents can be categorized based on a number of possible facets, including type of breach, level of potential harm and risk to the organization, level of expertise needed to perpetrate the incident, type of organizational structure (such as a V-CoP), and ease of detection by automated and human measures. Categories have been developed by a number of researchers in the cyber security field (Kjaerland, 2006). Each of these researchers looked at computer security incidents from a slightly different perspective. For example, one looked at the incidents based on the activities that the hacker was involved in, and another divided hackers into a spectrum of abilities. However, the most comprehensive collection of computer security incidents has been collected by CERT/CC (Computer Emergency Response Team/Coordination Center) at Carnegie Mellon University. CERT/CC collected 319,992 reported incidents from 1988-2003 (CERT/CC, 2004). Based on these incidents and focus on the com and gov domains, Kjaerland has come up with a new taxonomy (Kjaerland, 2006). It is worth noting that the majority of V-CoPs fall within these 2 domains and are therefore susceptible to the wiles of the hacker community.

Table 1 shows this new taxonomy that has been broken down into four facets: source sectors, method of operation (MO), impact, and target sectors. Source sectors refers to the source of the incident, or the sectors that attackers came from when attempting to attack a system. MO refers to the tool used to attempt the attack. Impact refers to the effect of the attack or what the attacker was trying to accomplish. Lastly, target sector refers to the victim of the incident or, in this case, the domain they can be found under. The majority of the attacks were aimed at com and gov target sectors.

Table 1 - A New Taxonomy (Kjaerland, 2006)

A new taxonomy (Kjaerland, 2006)			
Source sectors	Method of operation (MO)	Impact	Target sectors
Com Gov Edu Intl User Unknown	Misuse of Resources User Compromise Root Compromise Social Engineering Virus Web Compromise Trojan Worm Recon Denial of Service	Disrupt Distort Destruct Disclosure Unknown	Com Gov

Kjaerland (2006) found by analyzing the reported incidences that the most common type of incidence was root compromise, where the hacker gained access to the root of the system being attacked. Root attacks were the most common attack in both the com and gov target sectors. The com sectors reported root compromise for 35% of the incidences, with the next closest compromise being virus attacks at 26.5%. The gov sectors reported root

compromise for 25% of the incidences, with the next closest being web compromise at 22.5%, followed by reconnaissance (probing systems for weaknesses) at 14.8% and finally virus attacks at 13.8%. The most common type of incidence was root compromise followed by virus infections and or attempted attacks (Kjaerland, 2006; CERT/CC, 2004).

Root compromise is the most dangerous type of hack since the intruder has administrative access to the system being attacked. However, root attacks cannot be corrected by an end-user or a member of a V-CoP. For the purpose of this research, root compromise can be ruled out as a V-CoP member issue. The next most common type of incidence was virus attacks for com target sectors and fourth for gov sectors. The incidence types for gov after root compromise would also not be a V-CoP member issue but rather the responsibility of the system administrator. Members of a V-CoP would be more likely to encounter virus or phishing attacks which are targeted at the end-user. Phishing attacks take advantage of users' inability to discriminate between bogus and genuine web sites and the web sites' content (Kumaranguru et. al., 2007). In a V-CoP environment this may become an issue as members share documents that may become infected by a virus or if an attacker is able to gain access to the password protected section of the V-CoP the hacker may be able to cause damage, though not an end-user issue.

The primary focus then needs to be on the member or end-user of a V-CoP and what likely incidents may occur and how simulation and training can be used to help curtail computer security incidents. Computer viruses seem to be of primary concern since they are most common and easier to encounter in everyday email exchanges and when infected documents

are shared in a V-CoP. According to Dickinson (2005), "The often long delay between the time a virus attack is launched and its signature is distributed, results in hundreds of thousands of infected messages delivered to enterprise networks and communities of ISP users, prior to the availability of any protection from its deployment". Even though users alone cannot be blamed for innocently opening email attachments, they can be made aware of the potential threats and problems caused by viruses. If viruses are not detected and the user opens an email attachment, the outcome is that the infected messages will almost certainly result in hundreds of infected PCs. That translates into tens or even hundreds of thousands of dollars in desktop clean up costs for each virus outbreak at each corporation, and untold costs to consumers. An estimated rate of 900 million virally infected messages a day, from four to five serious virus attacks per month, makes that cost unacceptable. As a result, many companies and vendors are exploring preventive systems that can stop virus outbreaks before they happen and minimize any damage or cost (Dickinson, 2005).

Summary

The practicality of computer security depends upon a number of factors. However, user-error is the major cause of security breaches and incidents (Kjaerland, 2006). An organization must have a strong computer security policy that is enforceable and not cost prohibitive. If it is not reasonable or cost effective to implement a policy then it is useless, or at least the components that meet this specification are not of use (Schneider, 2000). What is

central to any security policy is the adherence to the policy by the end-user. Do they know enough about the policy and do they understand the risks of not adhering to the policy? A solid understanding of both the risks and rewards of proper adherence to the policy is essential to keeping information as secure as possible. Awareness and training are crucial to ensuring a safe and effective V-CoP.

Members of any virtual community, particularly a V-CoP, need to understand the security issues involved in modern day computer security. This includes the importance of proper password creation and retention, virus protection, proper identification of members of the community, and other parts of the information security policy. To this end, members of a V-CoP must be properly trained and tested to ensure that they not only understand the major security issues of any electronic system, but that they follow these policies. Von Solms acknowledged that users cannot be held responsible for security problems if they are not told what such security problems are, and what they should do to prevent them (Von Solms and Von Solms, 2004).

CHAPTER THREE: METHODOLOGY

Introduction

In V-CoPs, security is essential to ensure that proprietary and secret data is kept secure, and that computer infections do not enter the group and cause damage to the data that is part of the knowledge base or worse. Chapter 2 provided background information on the current issues with computer security and how viruses are the major end-user problem. What is needed is a model of training that uses training with simulation and follow-up testing to monitor members of a V-CoP to see if they are remaining vigilant toward risks and understanding and following the tenants of a traditional security policy of an organization and of a V-CoP. Deterrence theory was used as the underlying theory for educating users of potential security risks and threats. Deterrence theory will produce a greater level of awareness to these security risks and threats if the end user understands the risks and costs. As mentioned in Chapter 2, deterrence theory is based on the premise that computer hacks will be less likely to occur if there is the assumption by the hacker that they have a high probability of being caught, and that the punishment will be swift. Deterrence theory was applied in this research to show the user of technology, specifically users in a V-CoP, that lax security adherence can lead to severe repercussions for the users' organization. If users are made aware of the damage that can be done by not following proper security protocols, they should be deterred from not following them.

Furthermore, proper security awareness training, using simulated scenarios, may help to deter users from the mishandling of data and inadequate understanding and adherence to their organization's security policy and, if different, the security policy of their V-CoP. Additional benefits of this research include the demonstration of how to use simulation for training purposes in a V-CoP, and how simulation can be used to do follow-up training and testing in a V-CoP.

Computer security breaches and incidents are prolific and the primary causes are end-user carelessness and mistakes (Baker, 2008). In a V-CoP, the need to understand and learn proper security procedures is particularly necessary as the members may never interact personally and need to know if the people on the other end of electronic communications are who they say that they are and that they should have access to the data (Hakala, 2008). Furthermore, the members must also apply standard security policy procedures to all of their electronic interactions.

The purpose of the study was to see the difference between the results of initial training with simulated security scenarios and on-going security awareness training with simulated security scenarios with an experimental group and three control groups, with only two of the groups receiving the initial training with simulated scenarios on the security issues related to the policy and procedures of a V-CoP.

The rest of this chapter will cover the research study and details of the subjects that were used in this study.

Research Study

A unique opportunity existed at UCF Regional Campuses to conduct research using an existing V-CoP. UCF Regional Campuses currently works with faculty from seven different post-secondary institutions on curriculum alignment issues through a professional V-CoP site that enables members to upload files, share and comment on ideas, provide best practices, and hold discussions. The site, <http://www.curriculumalignment.ucf.edu>, is powered by the Confluence wiki system. The groups worked well for the research since they are divided into separate subject matter areas. The subject matter groups are a network organization since they are independent organizations that work on projects and processes (Powell, 1990). The groups meet physically on a semi-annual basis but the majority of the pre- and post-work is electronic communication through the web portal that contains both public and password protected sections for each subject matter area. The subject matter areas in the V-CoP are biology, chemistry, math, and physics. The groups consisted of faculty from the seven institutions that are involved in curriculum alignment and best practices within their subject matter area. Prior to recruitment of the subjects, Institutional Review Board (IRB) approval was required by the university to use human subjects in research. Appendix H contains the approval letter from the IRB to conduct this research.

Upon IRB approval, subjects were recruited and then randomly selected to the treatment group or one of the control groups so that there were similar numbers of users in each group. The random selection and placement of subjects from different disciplines into

groups labeled A, B, C and D for the experiment also helped to minimize potentially skewed results based on field of expertise. The pre-training test at the beginning of the research helped to assess the users' existing knowledge about information security and the components of a standard security policy.

The four groups answered some basic demographic questions prior to the beginning of the study (see Appendix A). Table 2 shows the schedule of the study. After the table, there is a detailed explanation of the events.

Table 2 - Timeline and Events for Research Study

Time Frame	Group A	Group B	Group C	Group D
Start	Demographic Questionnaire	Demographic Questionnaire	Demographic Questionnaire	Demographic Questionnaire
Start	Pre-training test	Pre-training test	Pre-training test	
1-2 weeks	Security Awareness Training with Simulated Scenarios and Post-training test	Post-training test	Security Awareness Training with Simulated Scenarios and Post-training test	
3 weeks	Security Training with Simulated Scenarios and Follow-up Testing	Security Training with Simulated Scenarios and Follow-up Testing		
6 weeks	Same as above	Same as above		
9 weeks	Same as above	Same as above		
10 weeks	Final Test	Final Test	Final Test	Final Test

Groups A, B, and C took an information security pre-training test to assess their existing knowledge and to be used as a baseline for future testing (see Appendix B).

Approximately 1-2 weeks after the pre-training test, Group A and Group C received awareness training on computer security issues with simulated security scenarios along with the potential impacts of improper security procedures. A web-based interactive training session on computer security, with simulated security scenarios, that follows the tenets of a standard security policy was delivered to Group A and Group C in an online web-based format (using a registered domain name www.tidnet.com/infosectraining). Each section of the tutorial presented proper computer security procedures with simulated security scenarios, followed by examples of potential risks and how these risks can ultimately impact the organization. The tutorial started out with an overview of information security in general and its importance, including examples of organizations that have been breached and the results of these breaches. Historical examples of failing to follow proper security protocols were used to educate and provide information to deter lax execution of security procedures. When users are made aware of the high costs and potential damage and harm that can be inflicted with such breaches, deterrence theory posits that they should be discouraged from making careless mistakes when securing their data.

The web-based training provided overall training on the security issues. It included proper virus protection and prevention, proper password creation and maintenance, document and information protection, social engineering prevention methods, physical control of

personal resources, proper internet usage, phishing, and other related information security issues.

After the training session with simulated security scenarios (tutorial) for Groups A and C, they were presented with 20 security questions which asked the subjects to respond to each question presented with what they thought was the most secure answer. Each alternative was ranked from 1 to 5; 1 being the least secure response, and 5 being the most secure response. However, the answers were randomized so that the test subjects were not able to follow a pattern if similar questions were encountered. Post-training test results were compared to the pre-training test results. The questions were different but assessed the same subject matter and objectives. Also, embedded in the training were simulated scenarios of emails that, if opened, popped up a warning message. At the end of the test, the end-users were notified of the next steps and thanked for their participation in the particular completed section.

At 3, 6, and 9 weeks, following the initial security awareness training with simulated security scenarios and the post-training test, Group A and Group B were presented with more computer security training with a simulated event and were tested to measure the effectiveness of the training. The control group responses were compared to those of the treatment group and to the previous control group test scores. The tests for each training session were different and included a simulated security event, such as a bogus email with an attachment, which when opened, popped-up a warning that the user would have been infected with a virus. These were embedded within the training so that firewalls and other security software did not flag or route the emails to the junk or spam mail folder.

Other simulated security scenarios included phishing attempts and social engineering attempts. An example of a phishing event was to try to get the members of either Group A or B to respond to an email that was asking for proprietary information. An example social engineering event was a simulated phone call to the subjects from someone pretending to be from the IT Department who asked for information that should not be revealed, such as a password or other sensitive information. Social engineering events were also embedded within the tutorial simulations.

An additional example was a simulated email environment where the user is asked to respond to an email coming from someone inside of their organization. If the user clicked on the attachment to the email, the file produced an error message that alerted the user to a virus infection. They were then asked to further respond to the scenario by providing information on how they would report the security breach using an ordinal scale put in the form of a multiple choice question (5 = most secure, 1 = least secure). Another simulated scenario was a request from an “apparent” member of the V-CoP who needed a secure document. The end-user would then have responded to the request by providing the document. The training and subsequent periodic testing was composed of other simulated scenarios like those mentioned above. Each simulated scenario was followed up by a series of questions that asked the subjects to determine the most secure response. The follow-up questions and the possible responses may be seen in Appendix B.

The topics presented in the initial training were based on the SANS Institutes security policy project (SANS.org, 2009). The initial training was estimated to last approximately 30-45 minutes. The timing was verified during the pilot-test and the test subjects responded that the time did fall between 30 and 45 minutes. Each topic covered in the tutorial consisted of a definition of the topic followed by the proper application of the definition. For example, a section on passwords included the proper definition of a strong password followed by examples of strong and weak passwords and some details on how hackers can easily crack passwords with readily available software. Table 3 lists the topics covered, the sub-topics, and the outcomes that were measured.

Table 3 - Topics to be Included in the Computer Security Tutorial

Topic	Sub-Topics	Outcomes to be Measured
Passwords	<ol style="list-style-type: none"> 1. Proper length 2. Composition of characters 3. Changing password 4. Definition of a strong password 5. Associated risks 	<ol style="list-style-type: none"> 1. Understanding of the importance of a strong password 2. Defining how often a password should be changed 3. Describe the potential risks associated with weak passwords
File sharing and management	<ol style="list-style-type: none"> 1. Types of documents. 2. Proprietary nature of document 3. Version management 4. Backups 5. Deleted and stolen documents 6. Legal issues 7. Ownership and control of data 	<ol style="list-style-type: none"> 1. Clear understanding of what documents should be shared and to whom 2. List the risks associated with sharing documents to unauthorized users 3. Define the potential penalties associated with sharing proprietary and confidential documents 4. Understand the responsibility and liability of the owner of the compromised data
Email Use	<ol style="list-style-type: none"> 1. Email security issues 2. Ownership of emails 3. Opening attachments 4. Proper identification of sender 	<ol style="list-style-type: none"> 1. Understand the risks associated with emails 2. Define the risks associated with opening attachments 3. List the proper way of identifying the sender of an email message 4. Financial impacts of improper email security
Virus prevention	<ol style="list-style-type: none"> 1. Types of viruses 2. Anti-virus software 3. Anti-virus definitions 4. Infected files 5. Preventing infection 6. Scanning files 7. Examples of damages caused by viruses 	<ol style="list-style-type: none"> 1. Understand the risks associated with out-of-date anti-virus software. 2. Know basic techniques to prevent virus infection 3. Identify suspicious web links in emails or on other web sites 4. Understand to do when a file or system is infected 5. Explain the potential financial and other damage causes by viruses

Table 3 - Topics to be Included in the Computer Security Tutorial (cont'd)

Phishing protection	<ol style="list-style-type: none"> 1. Definition of phishing 2. Phishing techniques 3. Potential risks 4. Examples of phishing attempts and their results 	<ol style="list-style-type: none"> 1. Define phishing and how it is used to compromise end-user security 2. Understand the risks associated with phishing
Data and data storage device disposal	<ol style="list-style-type: none"> 1. Importance of proper data disposal 2. Risks associated with improper data disposal 3. Deleting data from and destroying data storage devices 4. When to dispose of out-of-date data. 	<ol style="list-style-type: none"> 1. Understand the importance of proper data disposal 2. Identify risks that are associated with the improper disposal of data and data storage devices 3. List the proper techniques for deleting data from storage devices 4. Define when data should be disposed of and the legal issues surrounding data deletion
Social engineering	<ol style="list-style-type: none"> 1. Definition 2. Types 3. Ways it is used 4. Risks and examples 5. Ways to protect against 	<ol style="list-style-type: none"> 1. Recognize the proper definition of social engineering 2. List several types of social engineering 3. Understand the risks associated 4. List ways to protect against 5. Describe several different applications of social engineering
Work space security	<ol style="list-style-type: none"> 1. Proper security of data devices and systems 2. Security issues of the physical work space 3. Storage 4. Security of occupied and non-occupied work spaces 	<ol style="list-style-type: none"> 1. Understand the importance of proper work space security 2. List several different ways to secure the work space 3. Describe proper ways to store data 4. Define the difference strategies for securing an occupied and unoccupied work space
Mobile device security	<ol style="list-style-type: none"> 1. Securing laptops and other mobile devices 2. Password protection 3. Physical security issues 4. Data backup 5. Risks associated with compromised devices 	<ol style="list-style-type: none"> 1. Understand the importance of mobile device security 2. Describe why password protection is important 3. List physical security concerns for mobile devices 4. Define the steps taken when a device is stolen or compromised

At the end of the research period, and at each training and testing interval, the test answer data was analyzed and contrasted using the Kruskal-Wallis non-parametric ranked multi-group statistical test. It was assumed that the Group A had a more effective response rate to the testing and simulated security scenarios. The four groups were used to determine the effect that testing had on the control group with or without intermittent testing and training with simulated security scenarios.

The next section lists the research questions and hypotheses for this research study. After each time period, test data was collected and analyzed to determine if the null hypothesis, no significant difference, was rejected. If the null hypothesis was rejected, then we know that the training, with simulated security scenarios, did impact the security awareness of the treatment group.

Research Questions and Hypothesis

The focus of the research was on the impact that security awareness training using simulated security training and testing has on members of V-CoPs. Below are questions and hypotheses that relate to the training with simulated scenarios and testing that took place during the proposed research.

Initial training question

Will users who receive the security awareness training with simulated security scenarios show a positive significant difference in how they respond to the post-

training test on computer security in comparison to the users who received no training?

Initial training hypothesis

H_1 = Users who receive the security awareness training, Groups A and C, will show a positive significant difference in how they respond to testing and mock security events after the post-training test in comparison to the Group B.

Follow-up training question

Will users who received the security awareness training show a positive significant difference in how they respond to mock training with simulated scenarios and testing 3, 6, and 9 weeks after the training in comparison to the users who received no training?

Follow-up training hypothesis

H_2 = Users who receive the periodic security awareness training with simulated security scenarios will show a positive significant difference after 3, 6, and 9 weeks in how they respond to re-testing and periodic security training as compared to those who do not receive the periodic training and testing.

Final training question

Will users who received the security awareness training with simulated security scenarios show a positive significant difference in how they respond to the training and testing at the end of the training in comparison to the users who received no training?

Final training hypothesis

H₃ = Users who receive the security awareness training with simulated security scenarios and follow up testing (Group A) will show a positive significant difference at the end of the study on the final test as compared to the control Groups (B, C, and D).

The next section describes the data collection points and the kinds of data that was collected during the research study. At each interval, testing data was collected and analyzed to determine the impact of the training with simulated scenarios and testing on the subjects.

Data Collection and Instrumentation

The data collection began with a demographic survey (see Appendix A) followed by a pre-training test (see Appendix B). As mentioned in the previous section, there were four groups involved in the experiment. Group A was the treatment group; Group B was the control group who received pre-training tests, interval tests, and a post-training test. Group C was the control group who received only the pre-training test, training but no interval testing, and the final test at the end of the experiment. Group D received only the final test at the conclusion of training. Follow-up interviews were considered, but were not conducted since the results obtained from the groups or subjects were not skewed from the other subjects or groups. Appendix G has a listing of potential interview questions that could have been asked.

Test data was collected at all points along the testing cycles. Table 4 shows the various types of data that were collected at each of the testing points. The next section describes the data analysis techniques that were used.

Table 4 - Data Collected and Data Collection Points

Data Collected	Group A	Group B	Group C	Group D
Demographic Data Week 0	Data from all groups was collected. The collected data was specific enough to identify the individuals involved in the research. Appendix B contains the demographic questions that were used.			
Pre-training test Week 0	20 multiple choice questions were delivered to Groups A, B, and C. These were rated on an ordinal scale from 1 = least secure, to 5 = most secure.			No data was collected for Group D.
Initial simulated security training Post-training test Week 2	Subjects in Groups A and C received the initial simulated security awareness training. Groups A, B, and C took a post-training test comprised of 20 multiple choice questions similar in format to the pre-training test.			No training or testing was done for control Group D.
Simulated security testing and training Week 5	Groups A and B received additional security testing and training. Another test with 7 questions was delivered and rated just like the pre-training test.		No training or testing was done for control Groups C and D.	
Simulated security testing and training Week 8	Groups A and B received additional security testing and training. Another test with 7 questions was delivered and rated just like the pre-training test.		No training or testing was done for control Groups C and D.	

Table 4 - Data Collected and Data Collection Points (cont'd)

<p>Simulated security testing and training Week 11</p>	<p>Groups A and B received additional security testing and training. Another test with 7 questions was delivered and rated just like the pre-training test.</p>	<p>No training or testing was done for control Groups C and D.</p>
<p>Final test and potential interviews Week 12</p>	<p>Final test was delivered, containing the same questions as the pre-training test (20 multiple choice questions ranked 1-5), to all groups to assess what, if any, learning occurred due to the training, to testing alone, and to previous knowledge. Final test interviews were considered for subjects that had anomalous results in comparison to other subjects in the same group. These were not done.</p>	

Data Analysis

A pilot test (see Table 5) was run using volunteer student subjects. Students were offered extra credit to participate in the study for the course they were currently enrolled. A total of 13 students were recruited and placed in one group, but only 9 of the students completed all of the events. All of the pilot study subjects were run through the entire experimental system in a condensed time period. All subjects answered the demographic questions and then took a pre-training test. Immediately after the pre-training test, all subjects received the initial training with simulated security scenarios. After the initial training they then took a post-training test. All subjects received the periodic training and testing every week, and then at the end of 3 weeks, took the final test (follow-up interviews were not performed).

Table 5 - Pilot Test Time Line and Events

Time Frame	All Subjects
Start	Demographic Questionnaire
Start	Pre-training test
1 week	Security Awareness Training and Post-training test
2 weeks	Simulated security testing and training
3 weeks	Simulated security testing and training
4 weeks	Simulated security testing and training
4 weeks	Final test

The Kruskal-Wallis (KW) method (see Appendix D for an example of using the Kruskal-Wallis test) was used to analyze the pilot test data and final research test data and, to conduct an analysis of the hypotheses and null-hypotheses. For the periodic follow-up testing, the Wilcoxon Rank Sum test was used since the KW method requires at least 3 groups. The KW method makes the following assumptions: (1) Randomly selected groups – each group will be randomly selected from the four curriculum alignment V-CoP groups, with 2 faculty subjects from each subject-matter area, for 8 subjects per group (see Table 6 below); (2) Independence within each sample – each group was comprised of randomly selected subjects that were a combination of members from all subject-matter groups; (3) mutual independence across groups; (4) measurement scale that is ordinal or numeric – the measurement was based on an

ordinal scale of most to least secure (1 to 5); and (5) the selected groups' computed KW values are identical or else yield larger KW values than other groups (Newbold, 2009).

Table 6 - Number of Subjects in Each Group for the Full Research Study

Groups	Group A	Group B	Group C	Group D
Subject Matter Areas				
Biology	3 subjects	3 subjects	2 subjects	2 subjects
Chemistry	2 subjects	2 subjects	3 subjects	2 subjects
Math	2 subjects	2 subjects	2 subjects	2 subjects
Physics	1 subjects	1 subjects	1 subjects	2 subjects
Total	8 subjects	8 subjects	8 subjects	8 subjects

KW will tolerate groups of different sizes and the KW test procedure is approximately valid provided that the sample contains at least (5) five observations from each sample group (Newbold, 2009). Since the groups consisted of 8 subjects per group, the minimum number is slightly exceeded. Like many non-parametric tests, KW uses the ranks of the data rather than their raw values to calculate the test statistic. The KW non-parametric test makes no assumptions about the distribution of the data (Newbold, 2009).

The null hypothesis of the test was that all KW values are equal and the alternative hypothesis is that at least one of the groups yielded larger KW values than at least one of the other groups. If the test result was significant, multiple comparisons could be made between the samples. The comparison was based on a 0.05 level of significance with K-1 (K= number of

groups, so $K = 3$ for this study) degrees of freedom. All pairwise comparisons are made and the probability of each presumed non-difference is indicated.

Each group was presented with training and a variety of simulated training scenarios and appropriate follow-up questions. The hypothesis of the research was that Group A had a larger KW value than the other groups.

Test data was collected and analyzed after the initial testing to determine the difference between the results of the treatment and control groups. Then, one week after the initial training, Groups A and B received additional training with simulated scenarios and follow-up testing that included such items as an email that simulated an infection. If they clicked on the attachment, a message would be displayed on their screen saying that they should not have attempted to open the file, and other similar events based upon the initial training. This happened again after another week and so on until the test was complete. Group C and D received the final test at the end of the research.

The data was measured based on ordinal scoring for testing of the training with simulated security scenarios through general questions. The ordinal scoring was scored as follows: 5=best possible solution; 4=next best solution; 3=third best solution; 2=fourth best solution; 1=weakest solution. For each simulation presented, the subject responded to a series of questions based on the training to determine what solution the subject would pursue. For example, the user was asked to provide a password through a simulated email from their IT department.

The test data was then compared between the groups and a statistical analysis of responses based on training and no training was performed using the KW method. Once the data had been collected and ranked, comparisons were then made. Appendices C and D contain samples of data and how the data was to be compared at the pre-training test or post-training test levels. The assumption was that the pre-training test analysis was different from the post-training test analysis. The goal of the study was to see if the training had made a significant difference on the experimental group that received the training.

Summary

The overarching purpose of this research is to determine the efficacy and sustained benefit of information security awareness training using simulated scenarios to a V-CoP. The results of the study may provide useful feedback that organizations can use to determine if security awareness training using simulated scenarios in a web-based environment can help to reduce computer security incidences, particularly from viruses. Proper adherence to security guidelines should help to promote a safer environment. Also, when users are made aware of the risks and potential damages from viruses and other forms of computer security breaches that can occur when these guidelines are not followed, they should be more likely to follow these guidelines. Knowing the risks in any environment is helpful in producing desired responses.

Contributions to the field of computer security could be the longer term impact of training and retraining of members of a V-CoP. Other possible contributions would include the length of the training as it relates to retention of information security procedures and policies and the factor of simulated mock incidence events and how these events are handled by users who are exposed to computer security awareness training and users who are not. There has not been enough research into V-CoP and security and this research may lead to further studies being performed.

CHAPTER FOUR: ANALYSIS OF DATA

Introduction

The purpose of this research study was to determine the effect of information security training with simulated security scenarios and follow-up testing on the awareness of and the conformance to standard information security practices and policies within V-CoPs. The study was conducted over a twelve-week period during the summer of 2010. The subjects were college faculty members who participated in a V-CoP in curriculum alignment. The test data was collected through multiple web pages and web sites. Any data that required a response from the subjects was collected using SurveyMonkey, and all simulated scenarios and training information was delivered through www.tidnet.com, a private web site address. Demographic data and responses to test questions that followed the training and simulated scenarios was collected and then analyzed. Throughout the test data collection, subjects were emailed with instructions to access the simulated scenarios, training data, and follow-up testing.

This chapter discusses how the test data was collected and the test data collection tools that were used. Test data analysis techniques are explained, as is how the test data was analyzed in relation to the hypotheses.

Organization of Data Analysis

The test data collected are presented in sequential date order and by the research subject groups. First, the test data collected during the pilot study are presented and discussed. Then the test data collected for the full study are presented and discussed. Screen shots of each web page that was viewed by the subjects during the research study are also shown. Each section of the testing will be discussed along with the data that was collected throughout the testing, including:

- Pre-training test data for Groups A, B, and C (20 multiple choice questions),
 - Post-training test data for Groups A, B, and C (20 multiple choice questions),
 - Week 3 follow-up testing data for Groups A and C (7 multiple choice questions),
 - Week 6 follow-up testing data for Groups A and C (7 multiple choice questions),
 - Week 9 follow-up testing data for Groups A and C (7 multiple choice questions),
- and
- Final test data for Groups A, B, C, and D.

Presentation of Descriptive Characteristics of Respondents

Pilot Study

A pilot study was carried out to determine the efficacy of the training with simulated scenarios and follow-up testing. The pilot study included 13 students from 2 computer-concepts courses who were recruited specifically to test the functionality and usability of the

system. Only 9 students completed all of the components of the training and testing environment. These results were not analyzed for comparison or for statistical significance since all of the pilot-study participants were treated as one group and were presented with all parts of the simulated scenarios, training, and testing. The feedback from the pilot study was only positive. One pilot-study participant commented, “I feel that this was a great survey and I had learned a lot and recommend doing it again”, and another said, “This was very interesting”.

Table 7 shows the test data collected from the pilot study. The highlighted subjects did not complete all of the sections of the pilot study and their test scores are not included in the group totals. Student participants were able to successfully complete the training and each simulated training scenario without additional instructions or any other type of help. Each student was assigned a subject ID and password and they used this ID and password throughout the entirety of the pilot study. The participants who completed all parts of the pilot study were about equally spread between the two different courses and included 4 male and 5 female students.

The cumulative ranked scores increased slightly from the pre-training test to the post-training test, after the initial training with simulated scenarios, but essentially stayed the same as the pre-training test at the conclusion of the final test. The pilot study results are similar to the full study even though the educational levels of the subjects were different. This data was not analyzed and is presented to show that scores were created for the participants to make sure that they completed each section of the pilot-test (see Appendix B for test questions used in the pilot study).

Table 7 - Pilot Study Data

Pre-Test	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Sum of Scores
A2	a 5	c 3	b 3	a 5	d 5	e 1	b 5	a 5	c 5	e 5	a 3	d 5	b 5	d 4	d 5	a 5	b 4	c 3	c 3	c 3	82
A5	a 5	d 2	d 5	a 5	d 5	e 1	e 2	a 5	a 3	e 5	d 5	d 5	b 5	b 5	d 5	a 5	b 4	b 2	c 3	d 4	83
A6	a 5	c 3	d 5	c 2	d 5	c 5	b 5	a 5	c 5	c 3	d 5	a 4	d 4	b 5	a 3	a 5	d 1	e 5	c 3	e 5	80
B2	a 5	c 3	d 5	c 2	b 3	a 3	b 5	b 1	c 5	e 5	a 3	d 5	b 5	b 5	d 5	b 4	e 5	d 4	d 5	b 2	80
B4	a 5	c 3	d 5	a 5	d 5	e 1	b 5	a 5	b 4	e 5	d 5	e 3	d 4	d 4	d 5	a 5	c 3	c 3	a 2	e 5	80
B5	a 5	d 2	d 5	c 2	d 5	a 3	b 5	a 5	b 4	e 5	d 5	d 5	d 4	b 5	d 5	a 5	e 5	c 3	e 4	d 4	73
B6	a 5	d 2	d 5	e 3	d 5	e 1	c 3	a 5	c 5	a 4	d 5	a 4	b 5	b 5	e 2	a 5	d 1	e 5	e 4	d 4	75
C1	a 5	c 3	b 3	c 2	a 4	e 1	b 5	a 5	c 5	a 4	d 5	a 4	b 5	b 5	e 2	a 5	b 4	b 2	a 2	b 2	75
C5	a 5	d 2	d 5	b 4	a 4	c 5	b 5	d 4	a 3	e 5	d 5	c 1	b 5	a 1	d 5	a 5	c 3	b 2	c 3	c 3	75
C6	a 5	c 3	d 5	c 2	a 4	e 1	b 5	a 5	b 4	d 1	d 5	d 5	d 4	b 5	a 3	a 5	b 4	b 2	c 3	d 4	75
D1	c 4	c 3	e 2	d 1	d 5	a 3	e 2	e 2	c 5	e 5	d 5	d 5	d 4	b 5	a 3	b 4	a 2	c 3	a 2	c 3	89
D2	a 5	c 3	d 5	b 4	d 5	a 3	b 5	a 5	c 5	a 4	d 5	d 5	b 5	b 5	d 5	a 5	b 4	e 5	e 4	b 2	79
D4	a 5	d 2	b 3	b 4	d 5	e 1	b 5	a 5	a 3	e 5	c 4	d 5	b 5	e 2	b 4	a 5	e 5	c 3	d 5	c 3	79
Sub-Total:	45	25	39	30	40	21	45	40	39	35	40	37	42	36	37	44	33	29	30	29	716
Post-Test	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Sum of Scores
A2	a 5	c 3	b 3	a 5	d 5	e 1	b 5	a 5	a 3	a 4	c 4	a 4	d 4	b 5	d 5	a 5	c 3	b 2	c 3	d 2	76
A6	a 5	c 3	d 5	c 2	d 5	c 5	d 4	a 5	c 5	c 3	d 5	a 4	d 4	b 5	d 5	a 5	b 4	e 5	c 3	b 5	87
B2	a 5	c 3	d 5	b 4	a 4	e 1	b 5	a 5	c 5	e 5	a 3	d 5	b 5	e 2	a 3	b 4	a 2	e 5	d 5	b 5	81
B4	a 5	b 4	d 5	d 1	b 3	e 1	b 5	a 5	c 5	c 3	d 5	e 3	d 4	d 4	b 4	a 5	e 5	e 5	a 2	a 4	78
B6	a 5	d 2	d 5	c 2	d 5	e 1	c 3	a 5	e 1	c 3	d 5	a 4	b 5	e 2	a 3	c 1	c 3	b 2	a 2	b 5	88
C1	a 5	a 5	d 5	b 4	a 4	c 5	b 5	a 5	c 5	a 4	d 5	a 4	b 5	b 5	b 4	a 5	b 4	b 2	a 2	b 5	82
C5	a 5	b 4	d 5	c 2	d 5	e 1	d 4	a 5	c 5	e 5	d 5	a 4	d 4	e 2	d 5	a 5	b 4	b 2	d 5	b 5	74
C6	e 4	c 3	d 5	d 1	d 5	e 1	d 4	d 4	b 4	d 1	d 5	d 5	d 4	d 4	d 5	a 5	e 5	e 5	c 3	e 1	82
D1	a 5	c 3	e 2	c 2	a 4	d 4	d 4	d 4	c 5	d 1	e 2	d 5	b 5	e 2	b 4	b 4	a 2	c 3	d 5	e 1	93
D2	a 5	a 5	d 5	b 4	d 5	c 5	d 4	a 5	c 5	e 5	d 5	d 5	d 4	e 2	d 5	a 5	e 5	e 5	d 5	a 4	75
D4	a 5	b 4	b 3	c 2	d 5	e 1	b 5	d 4	c 5	e 5	d 5	d 5	d 4	e 2	d 5	a 5	e 5	b 2	a 2	e 1	75
Sub-Total:	44	34	41	25	41	21	41	43	42	35	42	39	38	31	41	44	37	33	30	32	734
Week3	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Sum of Scores													
A2	b 4	c 5	b 4	d 4	d 5	d 4	d 5	26													
A6	a 5	d 2	b 4	d 4	d 5	c 5	d 5	30													
B2	a 5	a 4	b 4	b 5	d 5	c 5	e 3	33													
B4	a 5	c 5	b 4	a 3	d 5	c 5	b 4	30													
C1	a 5	a 4	a 5	a 3	d 5	c 5	a 2	31													
C5	a 5	e 1	d 2	d 4	d 5	c 5	e 3	24													
C6	a 5	c 5	a 5	a 3	d 5	c 5	e 3	31													
D2	a 5	d 2	b 4	b 5	d 5	c 5	d 5	29													
D4	a 5	c 5	e 3	d 4	c 4	c 5	e 3	31													
Sub-Total:	44	33	35	35	44	44	33	265													
Week6	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Sum of Scores													
A2	d 5	d 2	d 3	a 5	e 3	d 5	d 5	23													
A6	d 5	a 5	b 4	d 4	b 4	d 5	d 5	32													
B2	d 5	a 5	e 2	a 5	b 4	b 4	d 5	30													
B4	d 5	b 3	d 3	c 3	b 4	d 5	d 5	28													
C1	e 4	a 5	a 5	d 4	b 4	d 5	b 3	32													
C5	d 5	d 2	d 3	a 5	a 5	d 5	d 5	28													
C6	d 5	a 5	d 3	a 5	a 5	e 1	a 4	29													
D2	b 3	d 2	d 3	e 1	b 4	b 4	d 5	21													
D4	d 5	c 4	d 3	d 4	a 5	b 4	d 5	30													
Sub-Total:	42	33	29	36	38	38	42	253													
Week9	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Sum of Scores													
A2	b 2	c 5	a 5	a 4	d 5	d 5	d 5	26													
A6	a 5	d 4	d 4	c 5	d 5	d 5	b 3	33													
B2	a 5	c 5	a 5	c 5	d 5	a 3	d 5	31													
B4	a 5	d 4	a 5	c 5	d 5	b 4	b 3	33													
C1	c 4	d 4	a 5	c 5	c 3	a 3	a 4	27													
C5	c 4	d 4	a 5	c 5	d 5	d 5	d 5	32													
C6	c 4	d 4	a 5	c 5	a 4	d 5	d 5	32													
D2	a 5	c 5	a 5	a 4	d 5	d 5	d 5	34													
D4	c 4	c 5	d 4	c 5	d 5	d 5	d 5	33													
Sub-Total:	38	40	43	43	42	40	40	281													
Final Post-Test	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Sum of Scores
A2	a 5	c 3	d 5	b 4	d 5	e 1	b 5	a 5	c 5	c 3	d 5	d 5	b 5	e 2	d 5	a 5	e 5	d 4	c 3	e 5	85
A6	a 5	c 3	d 5	a 5	b 3	c 2	b 5	a 5	c 5	c 3	d 5	d 5	d 4	b 5	d 5	a 5	e 5	e 5	c 3	e 5	88
B2	a 5	c 3	d 5	a 5	d 4	b 5	a 5	c 5	e 5	d 5	d 5	d 5	b 5	d 4	d 5	a 5	b 4	e 5	c 3	e 5	93
B4	a 5	c 3	d 5	b 4	d 5	b 2	b 5	a 5	c 5	a 4	d 5	d 5	d 4	d 4	b 4	a 5	e 5	e 5	a 2	a 1	83
C1	a 5	c 3	d 5	c 2	a 4	e 1	b 5	d 4	c 5	a 4	c 4	e 3	b 5	b 5	a 3	a 5	b 4	b 2	a 2	a 1	72
C5	a 5	c 3	d 5	c 2	d 5	c 5	b 5	a 5	c 5	a 4	d 5	d 5	d 4	e 2	d 5	a 5	e 5	b 2	c 3	a 1	81
C6	a 5	d 2	d 5	c 2	d 5	e 1	d 4	a 5	b 4	d 1	d 5	d 5	d 4	d 4	d 5	a 5	e 5	e 5	c 3	e 5	80
D2	a 5	d 2	d 5	c 2	d 5	e 1	d 4	e 2	c 5	e 5	d 5	d 5	d 4	e 2	d 5	a 5	b 4	e 5	c 3	b 2	76
D4	a 5	d 2	d 5	c 2	d 5	e 1	b 5	d 4	c 5	a 4	c 4	d 5	d 4	e 2	d 5	a 5	b 4	b 2	c 3	c 3	75
Sub-Total:	45	24	45	28	42	18	43	40	44	33	43	43	39	30	42	45	41	35	25	28	733

Full Research Study

Demographic Data

Demographic data and data on the computer experiences of the subjects was collected to determine if any differences in the subject groups might have led to differences in study results. Every subject in the study completed the demographic survey through the web interface SurveyMonkey.com. Table 8, on the following two pages, summarizes the demographic data collected with the responses organized by the four subject groups. Even though there was some variation between the groups, they were fairly homogeneous as one would hope following the random assignments to each group. For example, Group D had a higher ratio of men to women than any of the other subject groups and the most consistent age range (i.e., all members of Group D were between the ages of 40 and 59). The overall computer literacy of the subjects was higher than the normal everyday computer user, as evidenced by the number of computer courses taken and the exposure to virtual interaction through online course instruction and the interaction in a V-CoP. Lastly, the groups are fairly evenly distributed on the questions relating to anti-virus software, firewall installation, and uploading of files.

Table 8 - Demographic Data by Groups

		Groups	A	B	C	D
Question	Category	Options				
1	Male		4	3	4	2
	Female		4	5	4	6
2	Age	25-39	3	0	1	0
		40-59	3	5	4	8
		60+	2	2	3	0
3	Occupation	Faculty	8	8	8	7
		Staff	0	0	0	1
4	Subject	Biology	3	3	2	2
		Chemistry	2	2	3	2
		Math	2	2	2	2
		Physics	1	1	1	2
5	Education	Master's	2	4	3	3
		Doctorate	6	4	5	5
6	Number of Computer Classes Taken	None	1	0	0	2
		One	2	4	2	2
		Two	1	2	1	1
		Three	1	0	3	1
		Four or more	3	2	2	2
7	Types of Computer Classes Taken	Applications	4	4	5	2
		Programming	1	5	5	3
		Database	1	1	2	1
		Digital Media	3	1	1	0
		Other	3	1	1	3
8	Number of Computers Owned	None	0	0	0	1
		One	2	1	1	1
		Two	2	3	3	6
		Three	2	2	1	0
		Four or more	2	2	3	0
9	Computer Experience	Just learning				1
		Regular daily user	4	6	5	5
		Above average	3	2	2	2
		Expert	1		1	
10	How often Check Email	Hourly or more often	2	3	2	2
		About every 3 hours	4	2	2	4
		About every 6 hours	1	1	2	
		Twice per day	1	2	1	
		Once per day				2
		Less than once day			1	

Table 8 – Demographic Data by Groups (cont'd)

11	How often	Once per day	1			
	Use IM	Less than once day	2	1	3	
		Never	5	7	5	8
12	How often	More than once day	2	3	4	2
	Use Internet	Once per day				1
		Research	Every 2 or 3 days	3	3	1
		Weekly	1	1	2	1
		Monthly	2	1	1	1
13	Social	Yes	5	4	2	3
	Networking	No	3	4	6	5
14	What Social	Facebook	4	4	2	3
	Net Sites	Twitter	2		1	
15	Upload Files	Yes	7	6	5	5
	on Web	No	1	2	3	3
16	How often	More than once day	3	1	3	
	Upload Files	Once per day				
		on Web	Every 2 or 3 days	1	3	1
		Weekly	2	2	2	1
		Monthly	1		1	3
17	Anti-Virus	Yes	6	7	8	7
	Software	No	2	1	0	1
18	Anti-Virus	Yes	3	5	7	3
	Up to date	No	1	1		1
		Don't know	2	1	1	2
19	Firewall	Yes	6	8	7	7
		No	2		1	1
20	What Type	Software	1	3	2	1
	of Firewall	Hardware			1	
		Both	1	2	1	1
		Don't know	4		4	4
21	Computer	Yes	5	7	4	6
	Infected or	No	3	1	2	1
		Hacked	Don't know			2
22	Type of	Trojan	2	2	1	3
	Infection	Worm	3			
		Polymorphic	1			
		Don't know		2	4	4
23	Manage Own	Yes	3	2	2	2
	Web Site	No	5	6	6	6
24	Change	Monthly	1	1	1	
	Password	Every few months	4	5	4	3
		on Web Sites	Yearly		1	1
		Never	3	1	2	4

Research Questions and Associated Hypotheses

As each section of the data collection and analysis is presented, it must be done in the context of the research questions and hypotheses originally presented in Chapter 3.

Initial training

Will users who receive the security awareness training with simulated security scenarios show a positive significant difference in how they respond to the post-training test on computer security in comparison to the users who received no training?

First Research Hypothesis - Users who receive the security awareness training with simulated security scenarios, Groups A and C, will show a positive significant difference in how they respond to testing and security awareness scenarios after the post-training test in comparison to the control Group B.

Null Hypothesis – Users who receive the security awareness training with simulated security scenarios, Groups A and C will not show a positive significant difference in how they respond to testing and training with simulated security scenarios after the post-training test in comparison to the control Group B.

3, 6, and 9 weeks after initial training

Will users who received the security awareness training with simulated security scenarios show a positive significant difference in how they respond to the security training with simulated security scenarios and testing 3, 6, and 9 weeks after the training in comparison to the users who received no training?

Second Research Hypothesis - Users who receive the periodic security awareness training with simulated security scenarios, Groups A and B, will show a positive significant difference after 3, 6, and 9 weeks in how they respond to re-testing and the training with simulated security scenarios as compared to those who do not receive the training and testing.

Null Hypothesis - Users who receive the periodic security awareness training with simulated security scenarios, Groups A and B, will not show a positive significant difference after 3, 6, and 9 weeks in how they respond to re-testing

and periodic security training with simulated security scenarios as compared to those who do not receive the training and testing.

10-weeks after initial training

Will users who received the security awareness training with simulated security scenarios show a positive significant difference in how they respond to the training with simulated training scenarios and testing at the end of the training in comparison to the users who received no training?

Third Research Hypothesis - Users who receive the security awareness training with simulated security scenarios and follow-up training and testing, Group A, will show a positive significant difference at the end of the study on the final test as compared to the control Groups B, C, and D.

Null Hypothesis

Users who receive the security awareness training with simulates security scenarios and follow-up training and testing, Group A, will not show a positive significant difference at the end of the study on the final test as compared to the control Groups B, C, and D.

Data Collection Process

All 32 subjects successfully completed all parts of the study that they were expected to complete resulting in no missing data. Each subject was directed to the security awareness training with simulated security scenarios web site (see Figure 1) to begin the training and the testing for the research. The subjects were given a username and password that corresponded to their respective group (A, B, C, or D). After logging in to the web site, the subjects were then immediately directed to the demographic survey page (see Figure 2).

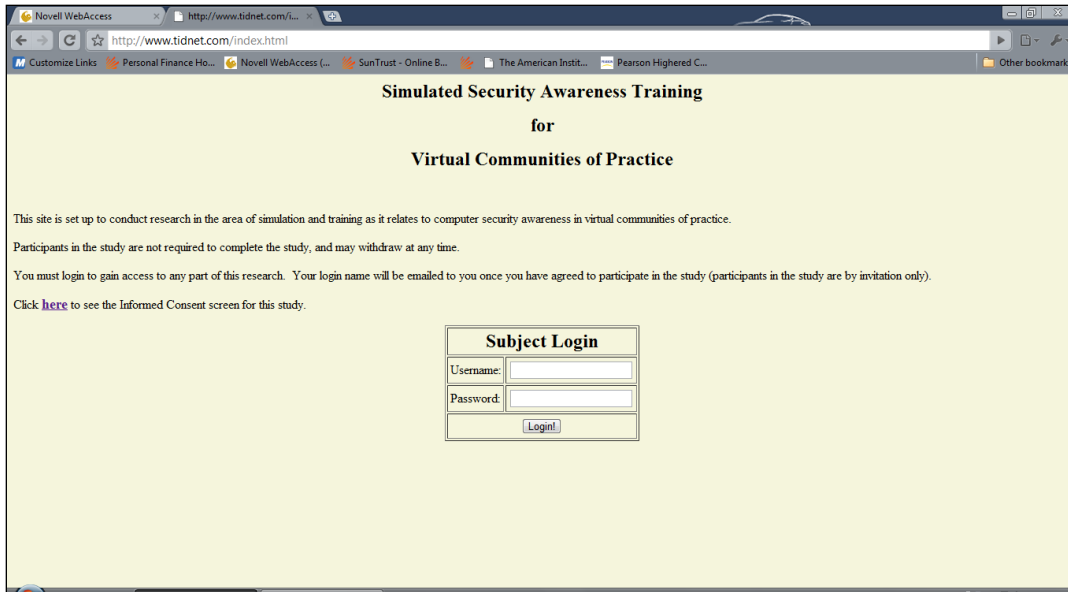


Figure 1 – Initial Login Screen for All Groups

The demographic survey page was hosted at SurveyMonkey and the subjects were transferred from the initial login screen to the demographic survey. The use of the SurveyMonkey site was transparent to the subjects. Each subject was given a unique subject ID which was based on his/her group. For example, Subject 1 one in Group A was given the subject ID of A1 to be used throughout all of the events that required a login. The subject IDs also ensured that the data was kept anonymous if it were discovered or compromised.

After the participants completed the demographic survey, they were then directed to the next screen (see Figure 3) which thanked them for taking the demographic survey. Groups A, B, and C were directed to the pre-training test screen (see Figure 4) and Group D was not.

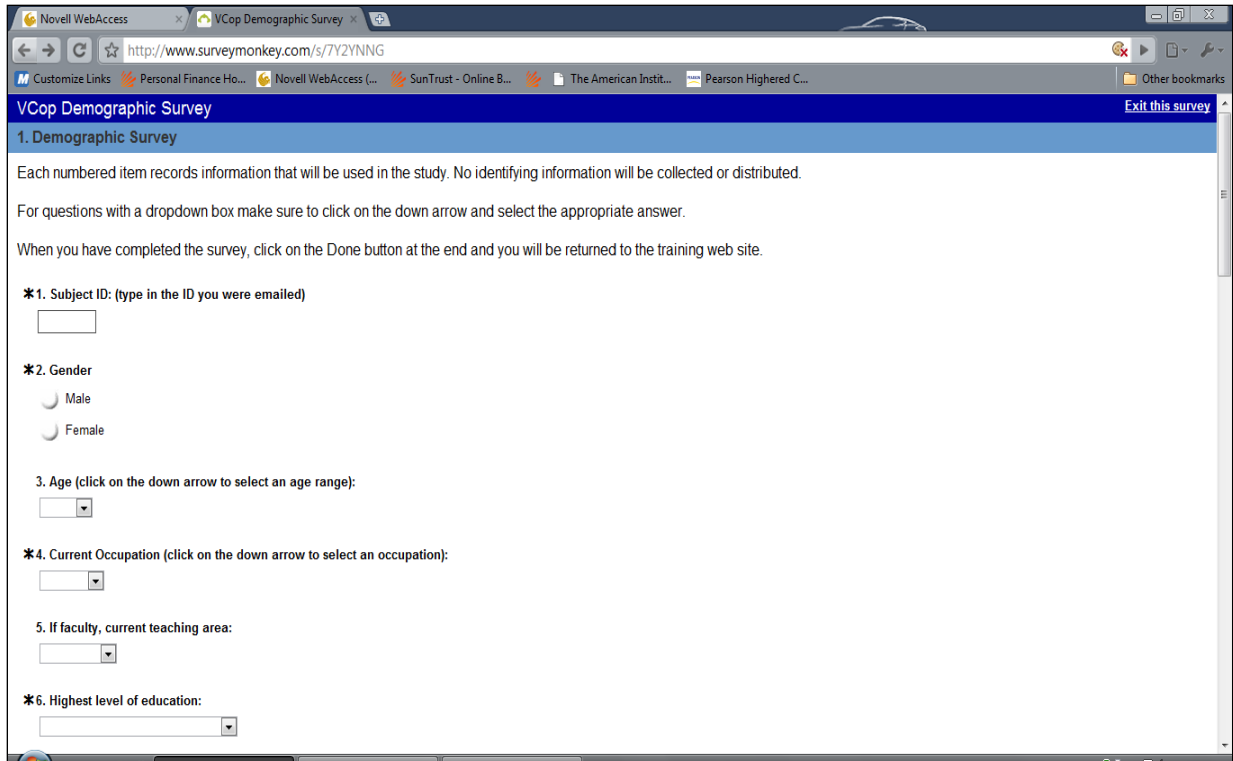


Figure 2 – Demographic Survey Screen

Figure 3 was just a brief thank-you screen that introduced Groups A, B, and C to the pre-training test page. Group D received the same thank-you screen but did not have the “Click here to continue: [Pre-training test](#)” link. Subjects in Group D were just told that they would receive more information in the future on the next steps of the research study.

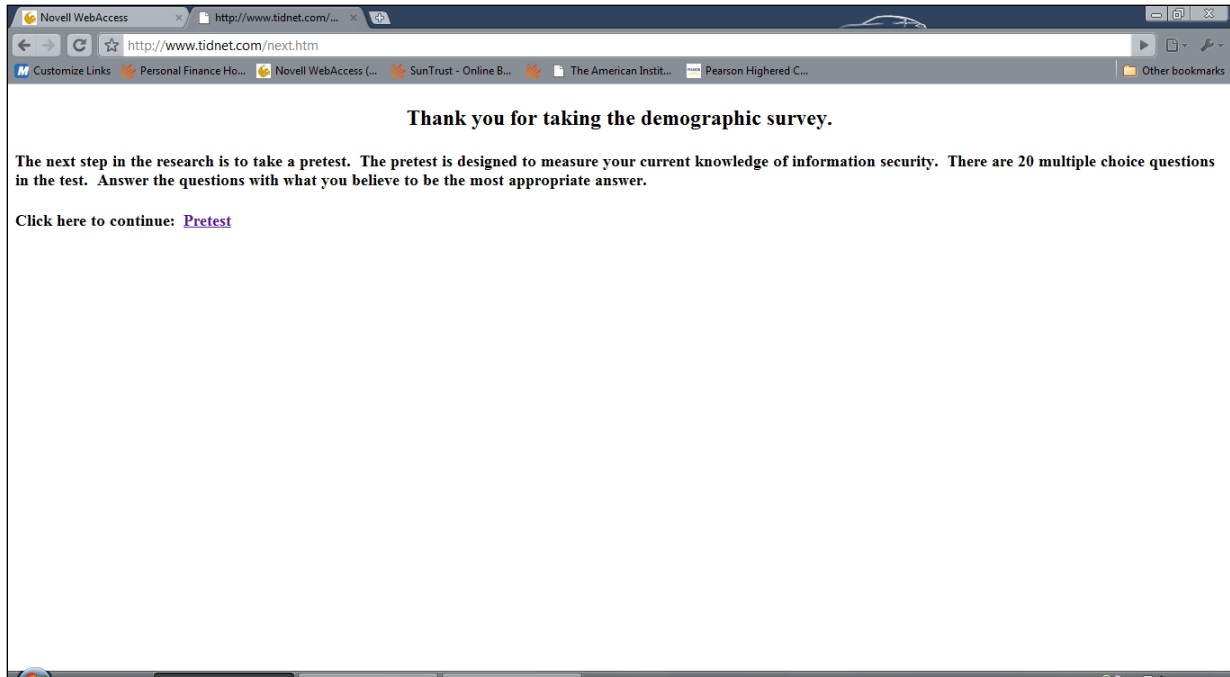


Figure 3 – Screen after Demographic Survey Completion

Once the subjects clicked on the pre-training test link, they were then taken to the screen shown in Figure 4. The pre-training test contained 20 questions that evaluated the information technology security literacy of the subjects. Groups A, B, and C answered the same questions, and this data was collected and analyzed using the Kruskal-Wallis test to determine if any initial difference existed between the three groups. After completion of the pre-training test, Groups A and C were then directed to the security awareness initial training site (see Figure 5) and completed the initial training with simulated scenarios. Group B was directed to a web page that thanked them for taking the pre-training test and informed them that they would be contacted in the future for further requirements of the research study.

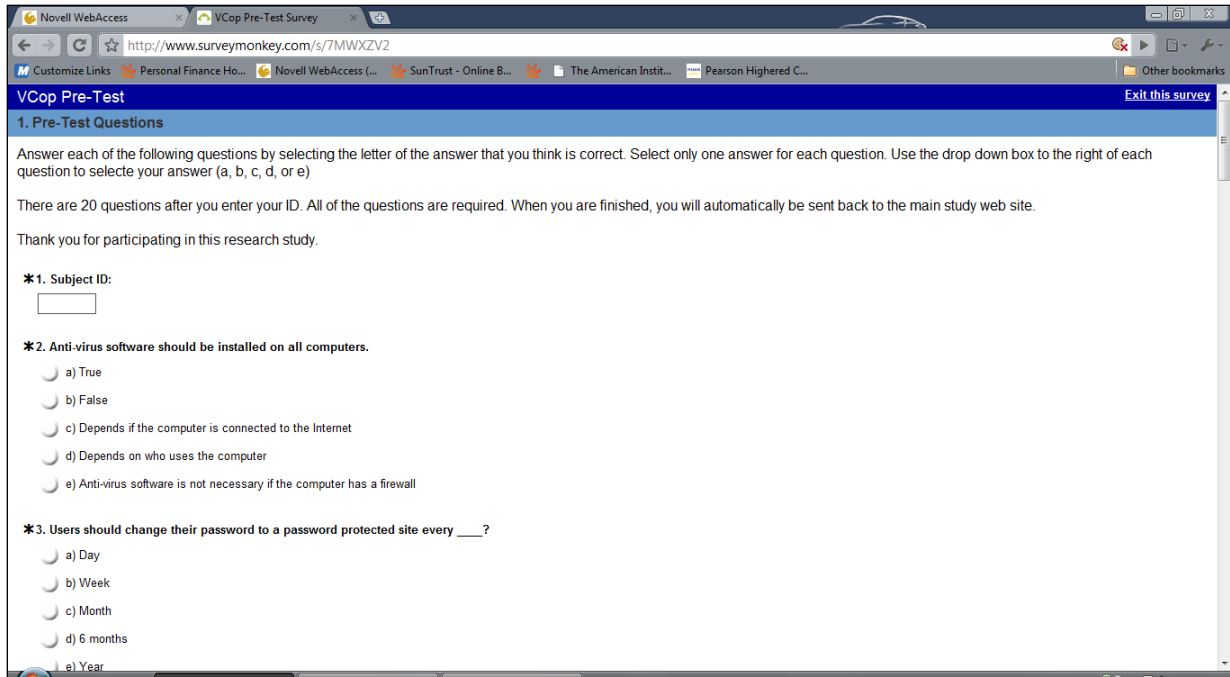


Figure 4 – Pre-training Test Screen

Figure 5 shows the screen of the initial security awareness training with simulated scenarios for Groups A and C. The training consisted of multiple sections and Figures 5 through Figure 18 shows all of the screens. The first screen consisted of information letting the subjects know what they would be seeing and approximately how long the training and testing would take. After the initial screen, the subjects were shown two more screens of information about information security (see Figures 6 and 7). Figure 6 included general information on computer security, and Figure 7 contained examples of security breaches that were included to reinforce the concept of using deterrence theory as a method of stimulating users to use sound information security practices.

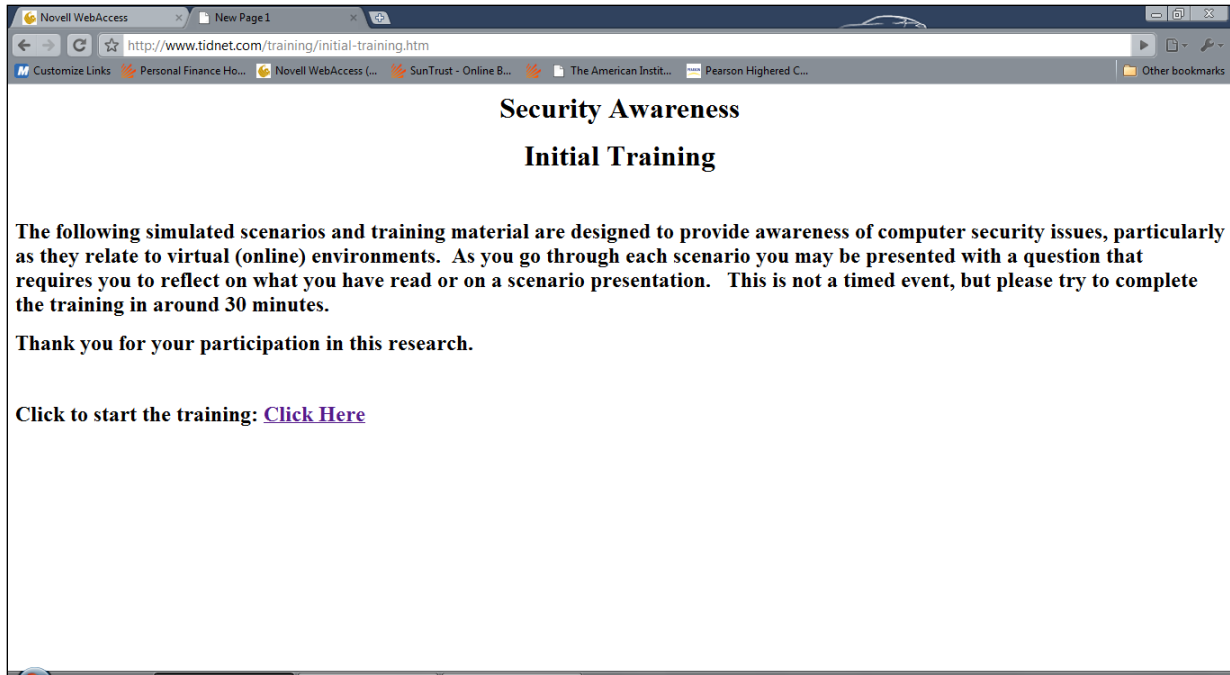


Figure 5 – Initial Security Training Introduction Screen

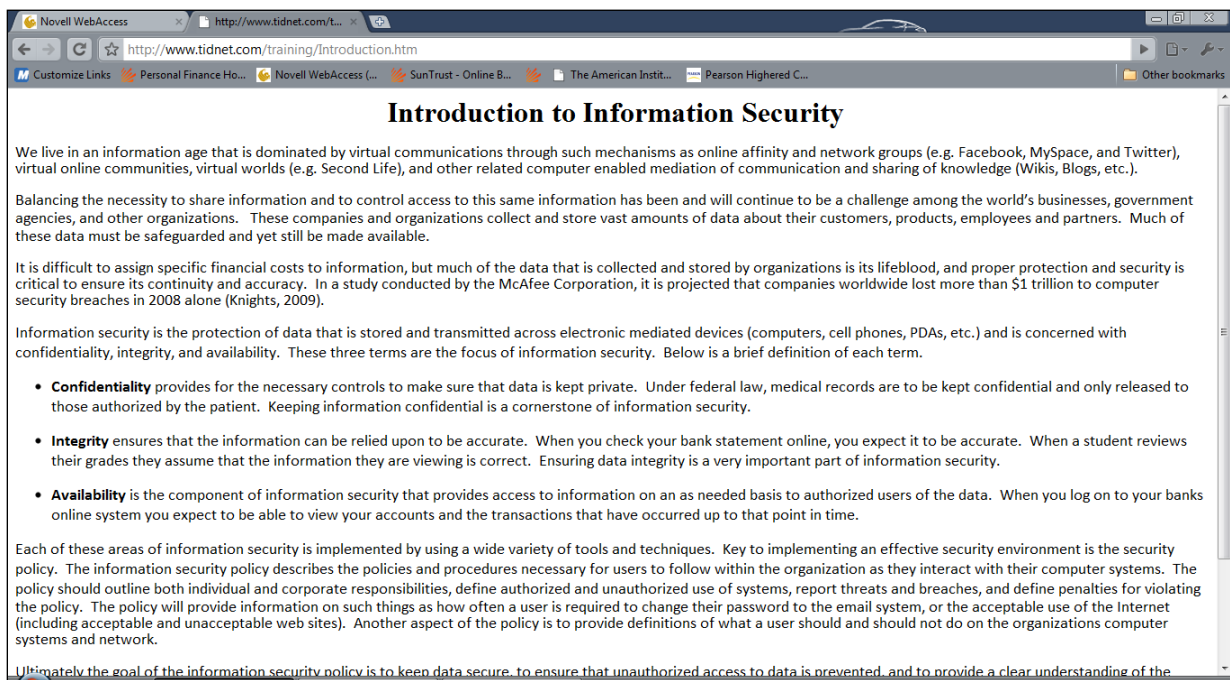


Figure 6 – Initial Training Overview Screen 1

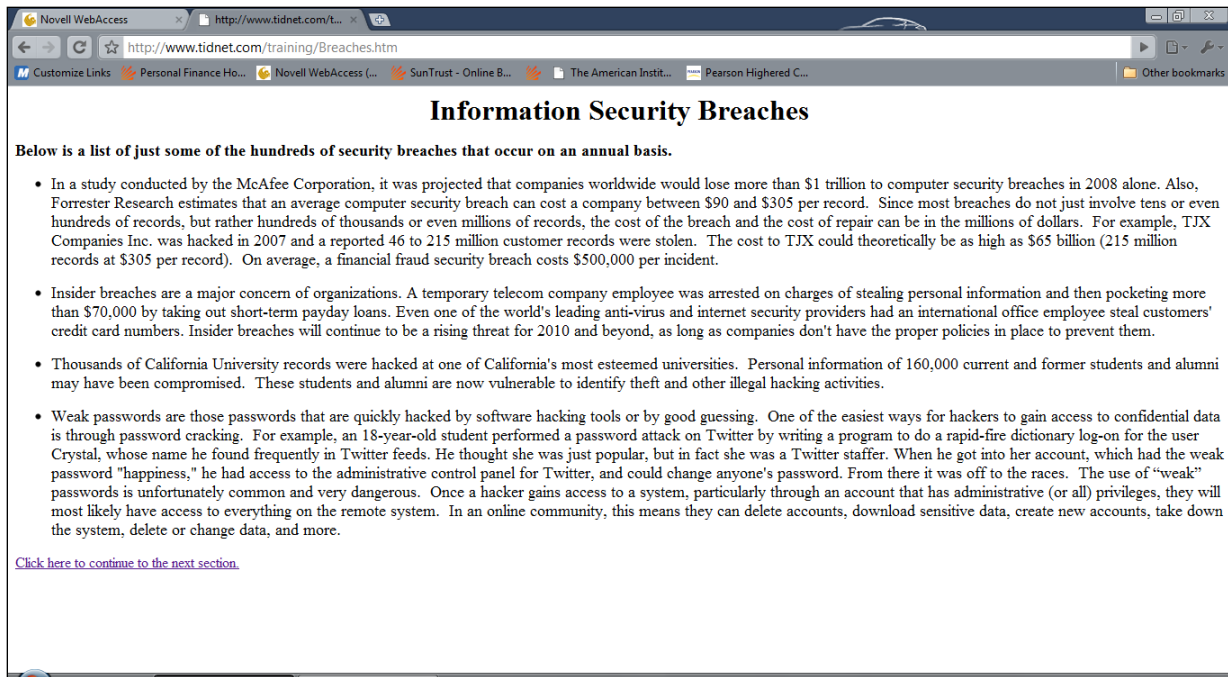


Figure 7 – Initial Training Overview Screen 2

Figure 8 included one of the first simulated scenarios in the training. The simulation link directed users to the Microsoft password simulation website (see Figure 9) where users entered either their own passwords or experimented with password samples to see the difference between a weak and strong password. This site was opened in a new window so that the subjects would not get lost or out of order when they were moving through the training web pages.

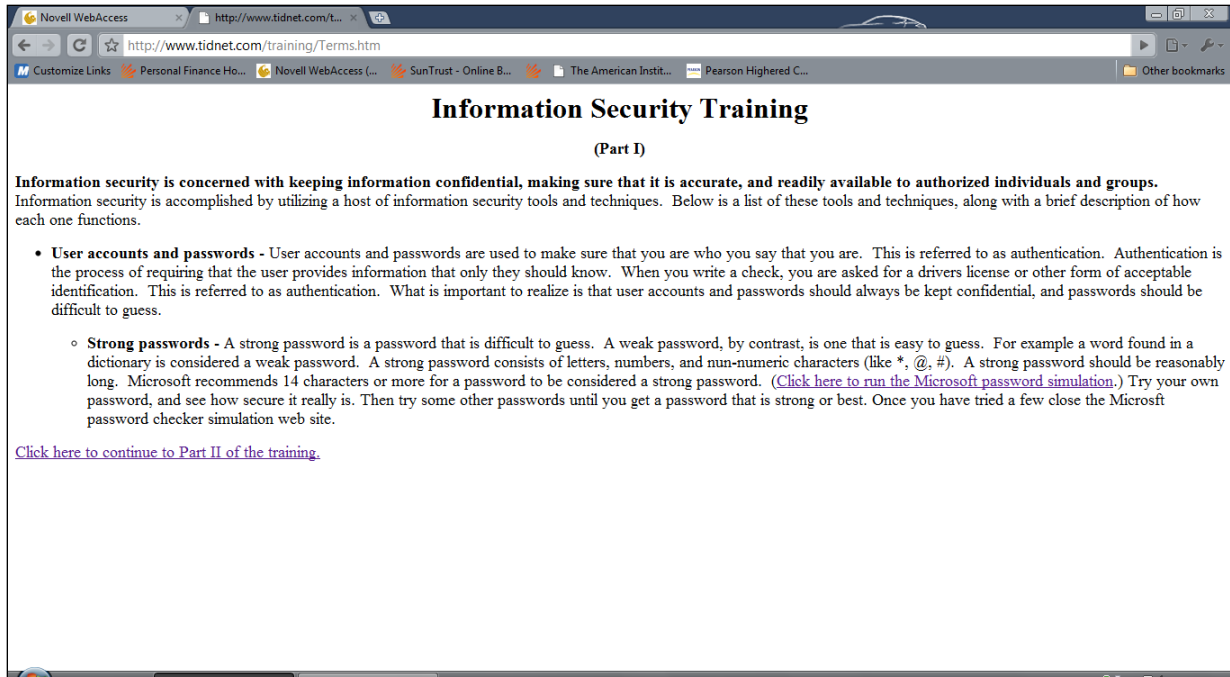


Figure 8 – Initial Training Part I

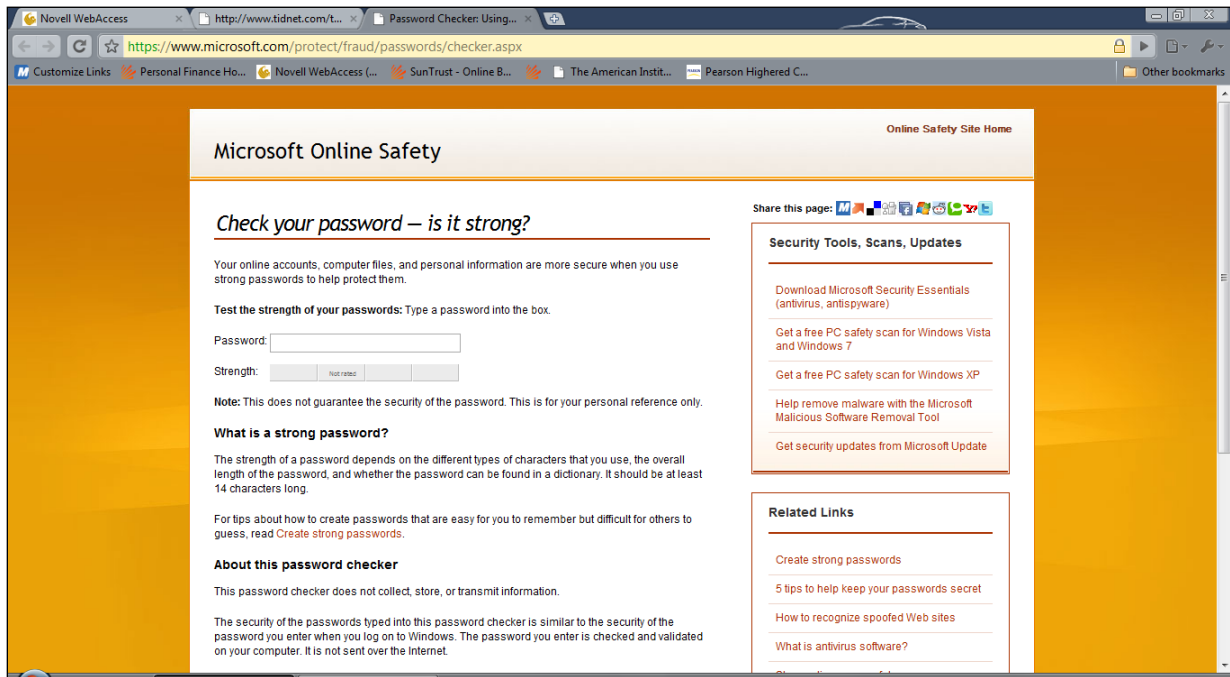


Figure 9 – Password Checking Site

After the subjects concluded the Microsoft password site, they were directed to Part II of the security training. Part II included two subject areas, file sharing and management, and email use (see Figure 10). Each section contained a link to a simulated scenario that required the subject to respond to a simulated file sharing scenario (see Figure 11) and to an email with a potentially virus-infected file (see Figure 12). Depending on how the subject responded to the scenario determined whether they received positive or negative feedback.

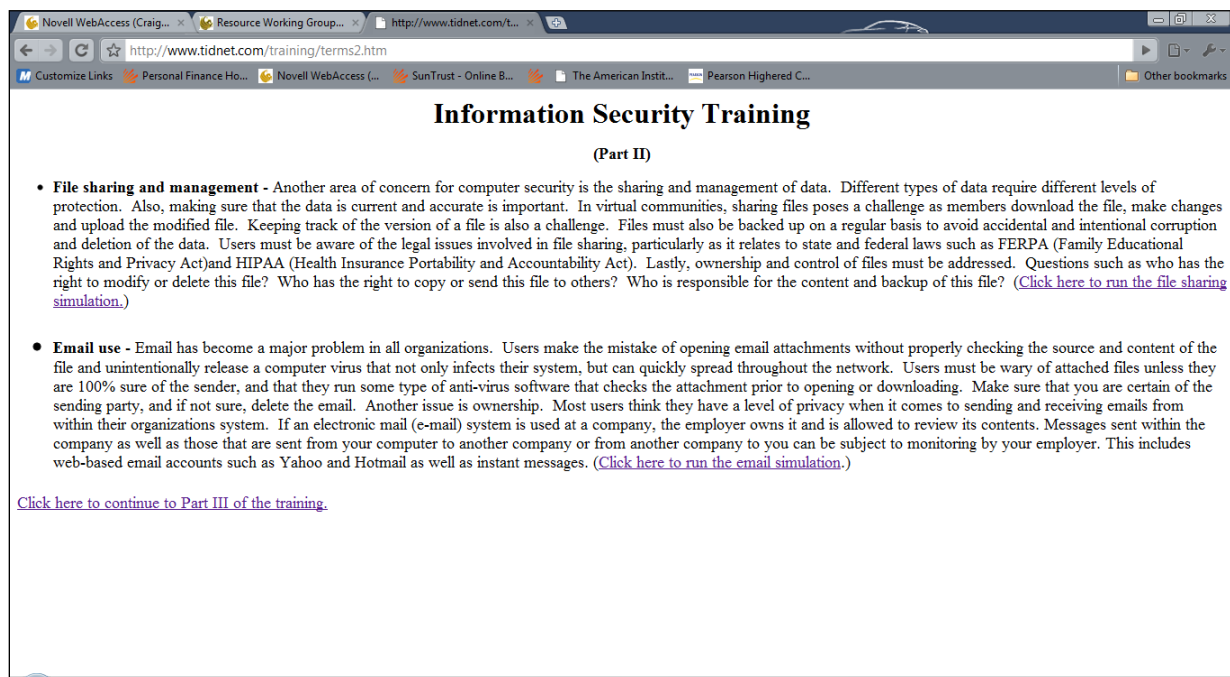


Figure 10 – Initial Training Part II

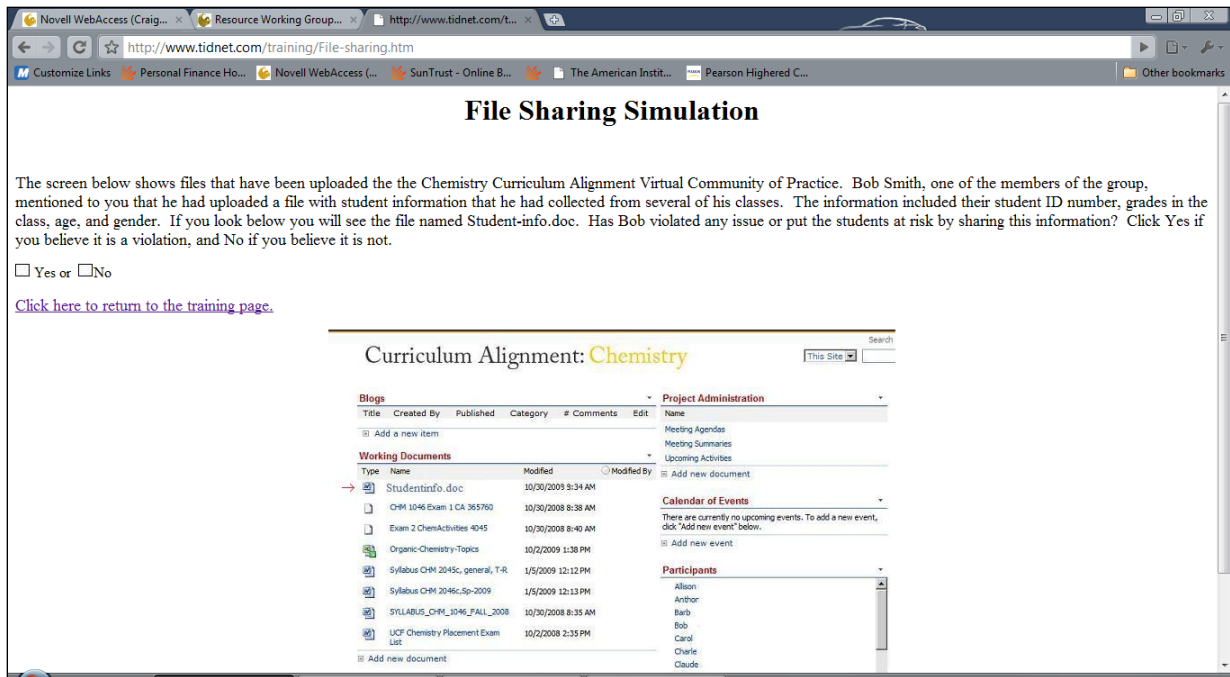


Figure 11 – File Sharing Simulation

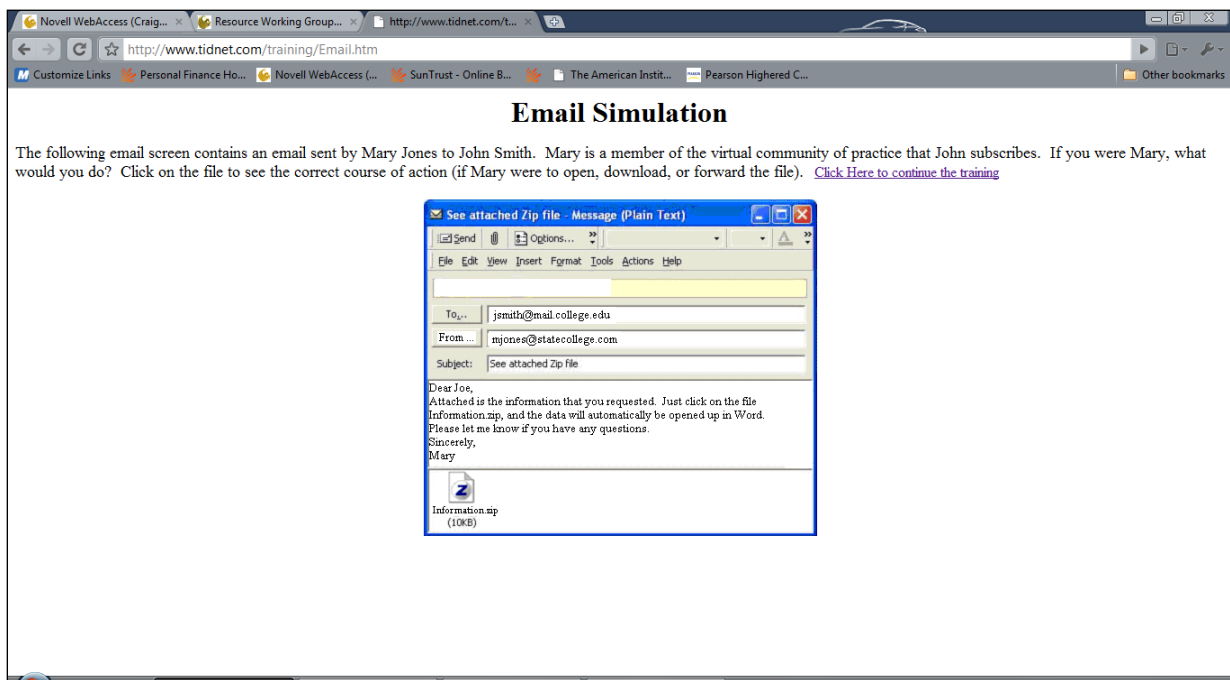


Figure 12 – Email Simulation

Next the subjects were taken to Part III of the training as shown in Figure 13. Part III covered virus prevention and phishing attacks. The virus prevention section contained a link from the email virus section to a simulated scenario. Figure 14 shows the email virus simulation, and Figure 15 shows the phishing simulation. The virus simulation presented the subjects with a screen from the V-CoP with a file that they should not download. The screen asked them to download the file and if they clicked on the file they were presented with a warning screen that discussed why they should not have tried to download the file. The phishing simulated scenario in Figure 15 tried to get the subjects to click on a link to go to another page. If they were not paying attention, they would click on a link that would take them to a bogus site that would seek to gather further information from them. The link is spelled incorrectly and, if they did not notice this they received further information on why they should not have clicked on the link.

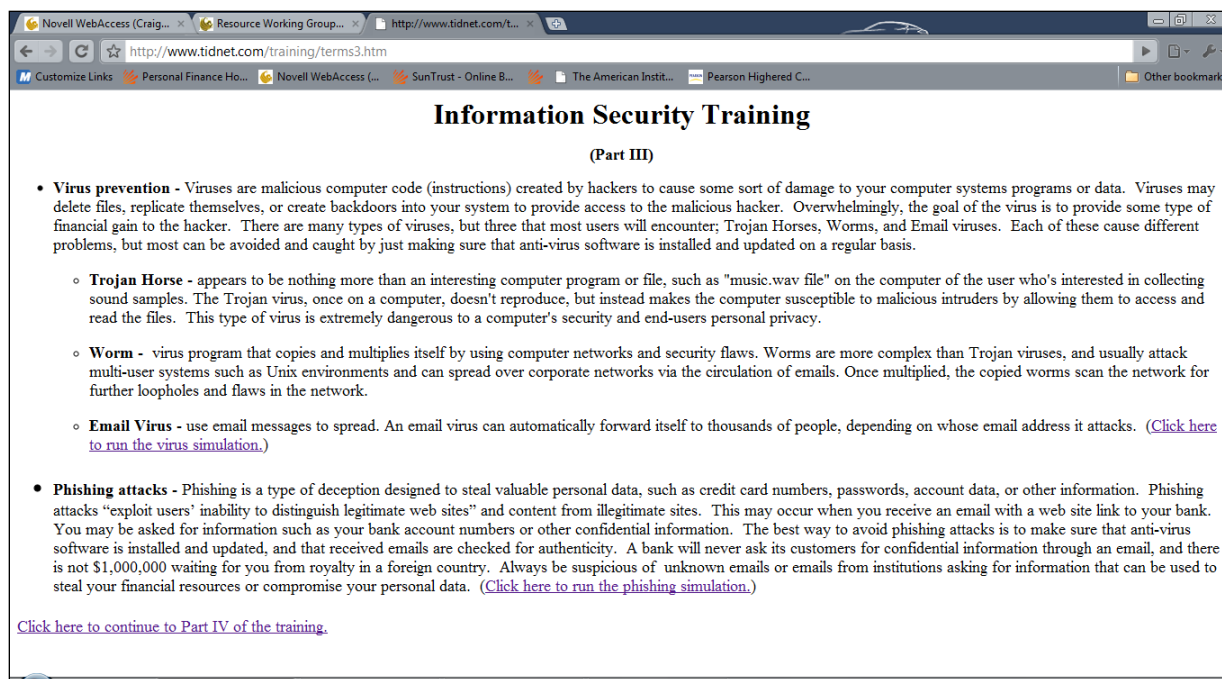


Figure 13 – Initial Training Part III

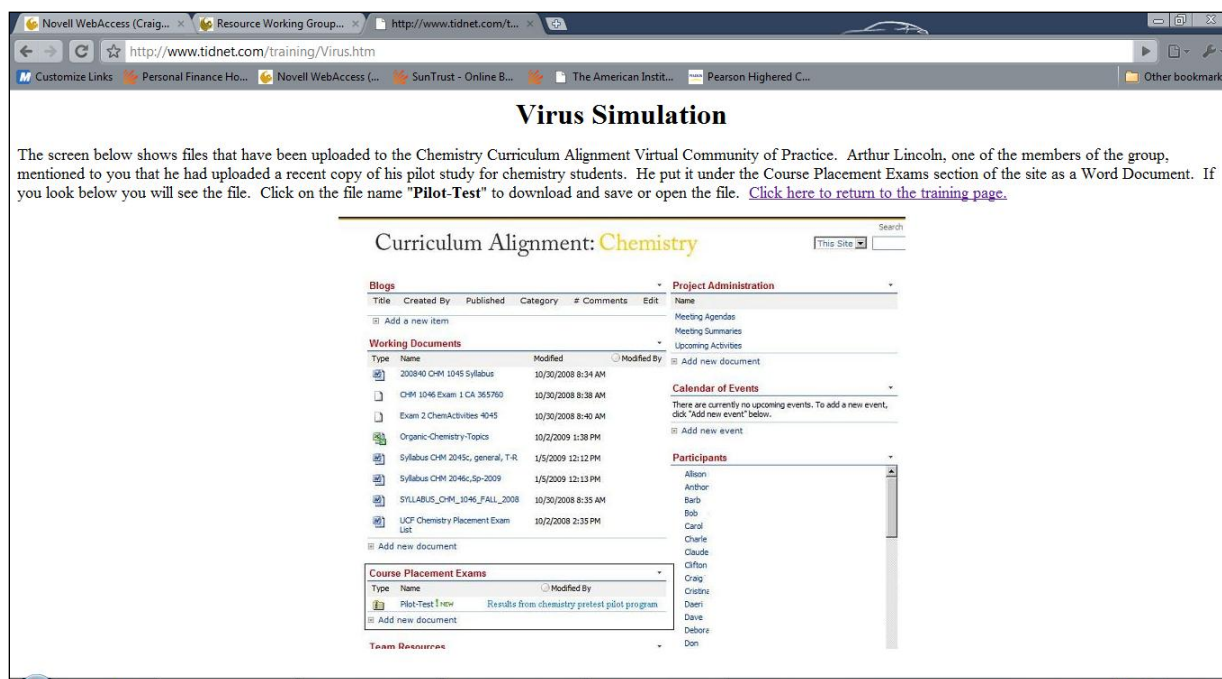


Figure 14 – Virus Simulation Screen

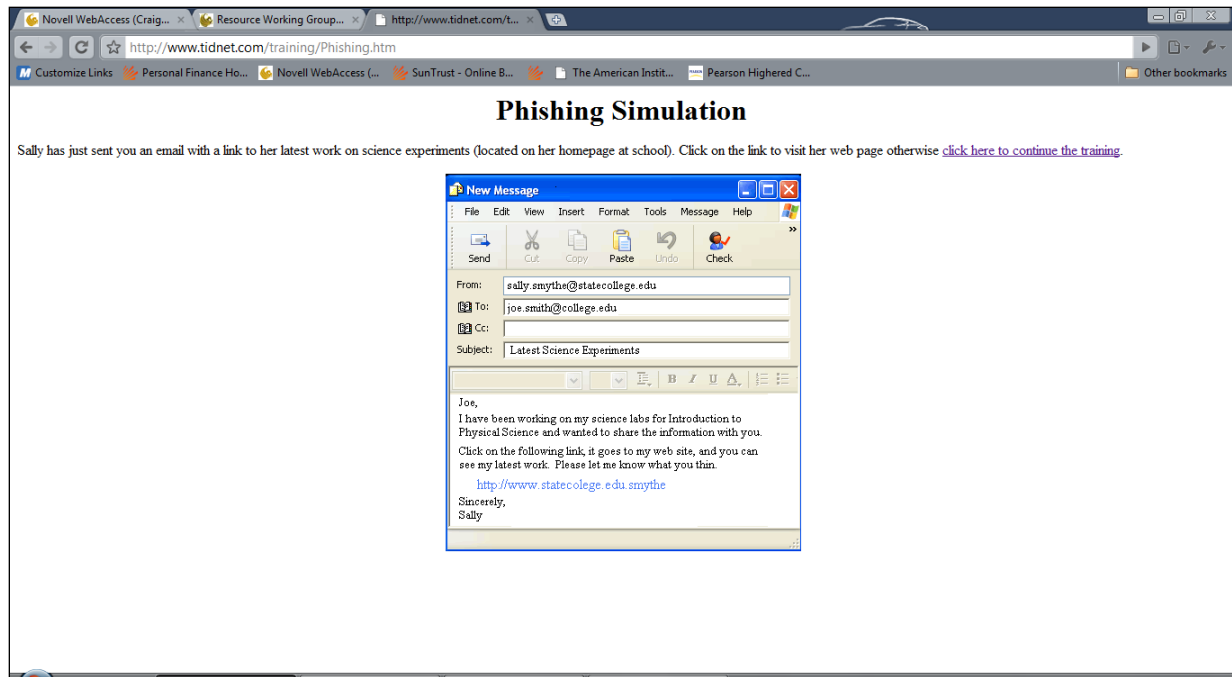


Figure 15 – Phishing Simulation Screen

Part IV (see Figure 16) of the training covered the last four sections of the information security training. This section covered data and data storage device disposal, social engineering, work space security, and mobile device security. The only part that contained a simulated scenario was social engineering since this part was most relevant to V-CoPs. Figure 17 shows the social engineering simulated scenario. This simulation played a recorded message coming from a supposed member of the IT Department. If for some reason their system did not play the message the subjects had the option of clicking on a link that would have shown the recorded message in a text box on the screen. They were then asked to respond to the recorded message by clicking on “yes” or “no” if they thought that they should provide the

information requested. After the simulated scenario, the subjects were directed to the conclusion screen of the initial training as shown in Figure 18.

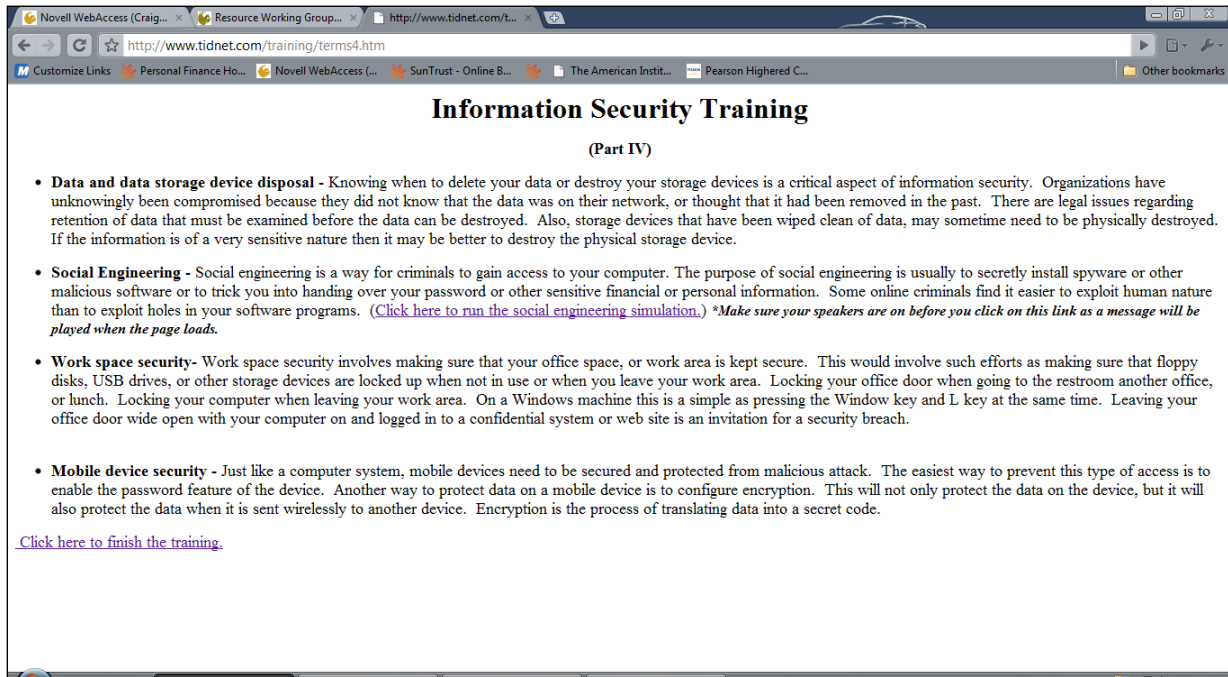


Figure 16 – Initial Training Part IV

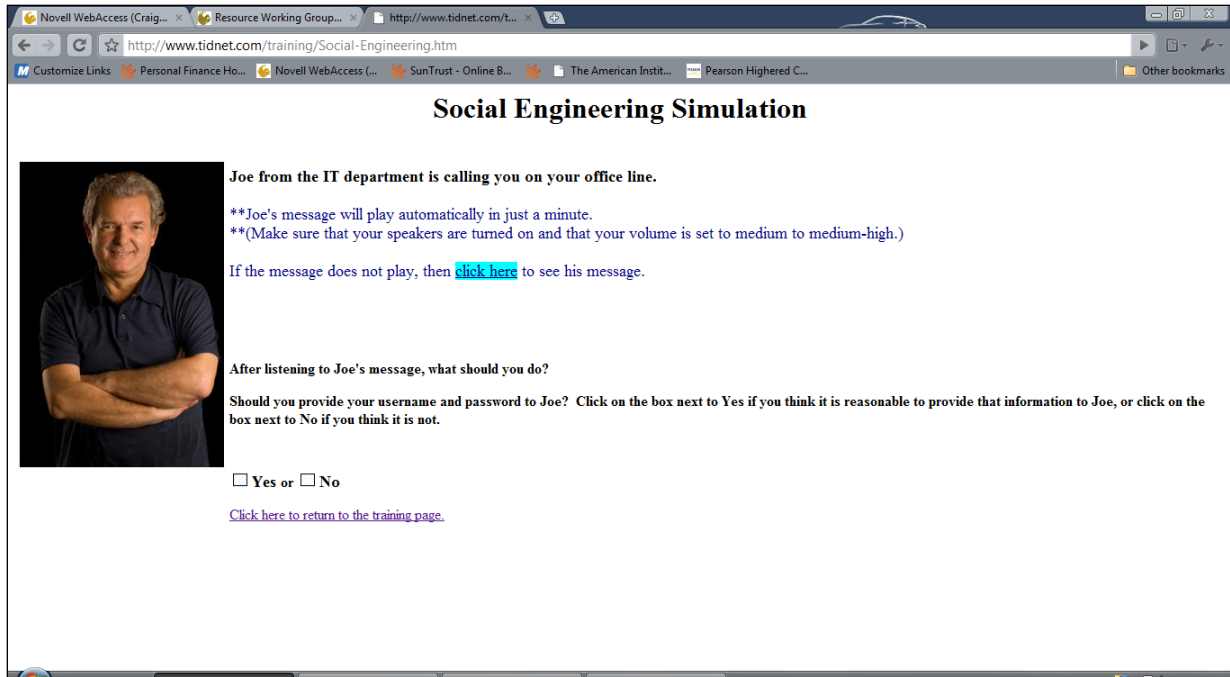


Figure 17 – Social Engineering Screen

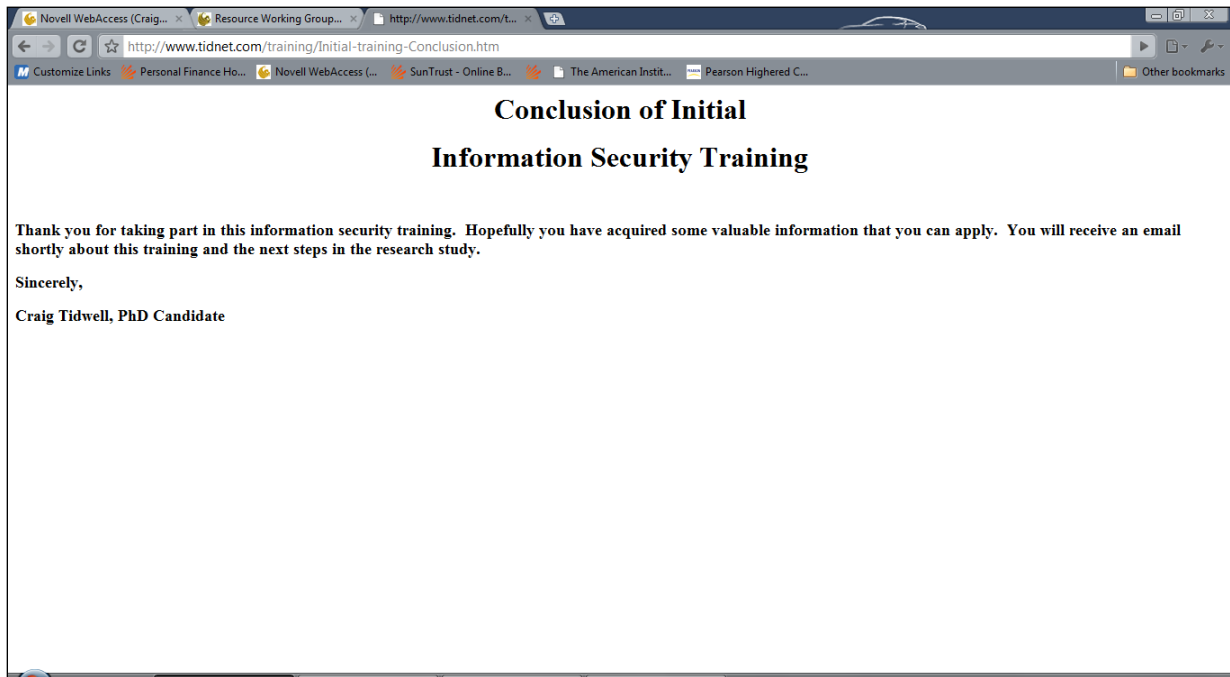


Figure 18 – Initial Training Conclusion Screen

Approximately one week after the conclusion of the pre-training test, subjects from Groups A, B, and C were sent an email with a link to the post-training test as seen in Figure 19. This page explained to the subjects that they would be taking an information security test with 20 questions. The post-training test consisted of questions that covered the same topics as the pre-training test. The test data collected is presented in the next section for the pre- and post-training tests. After completion of the post-training test, the subjects were taken to another thank-you screen as shown in Figure 21 and informed that they would be contacted in the future for upcoming events.

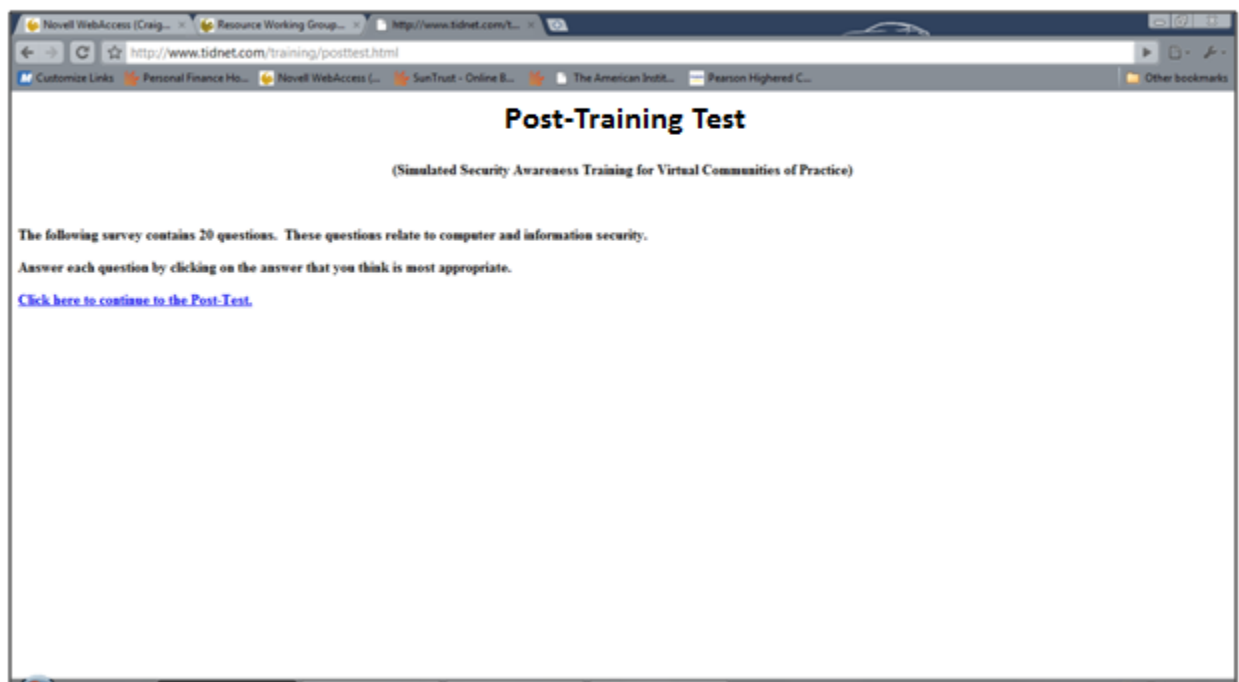


Figure 19 – Post-training Test Initial Screen

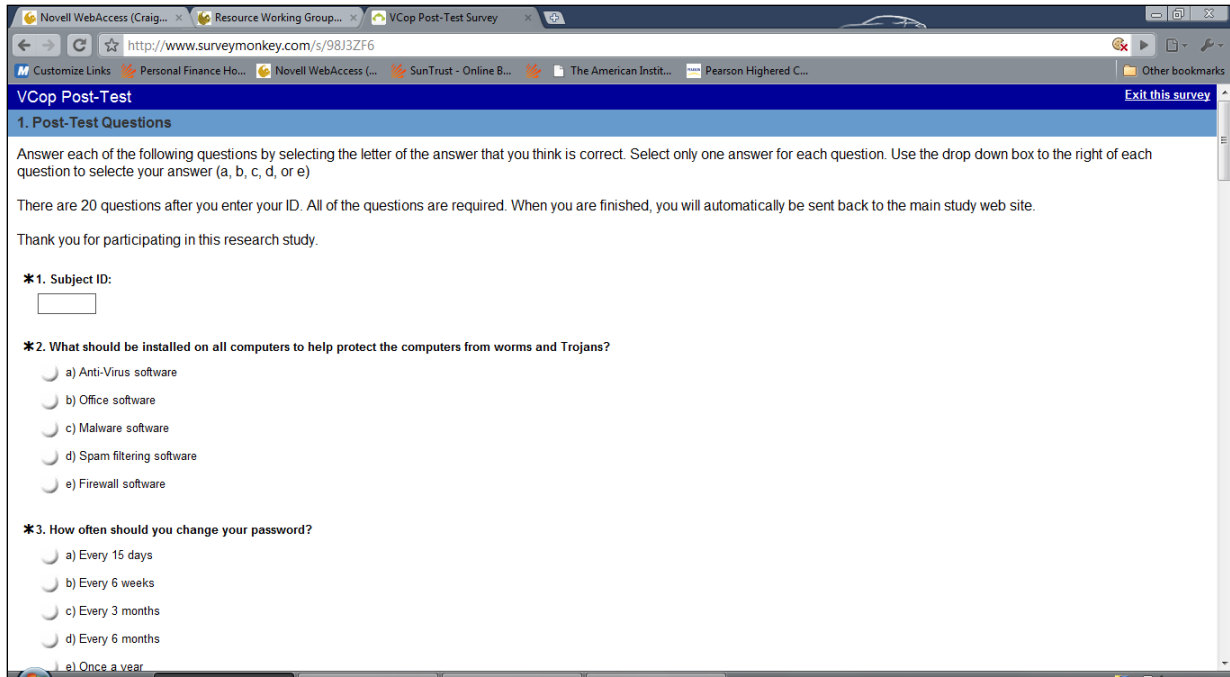


Figure 20 – Post-training Test Screen

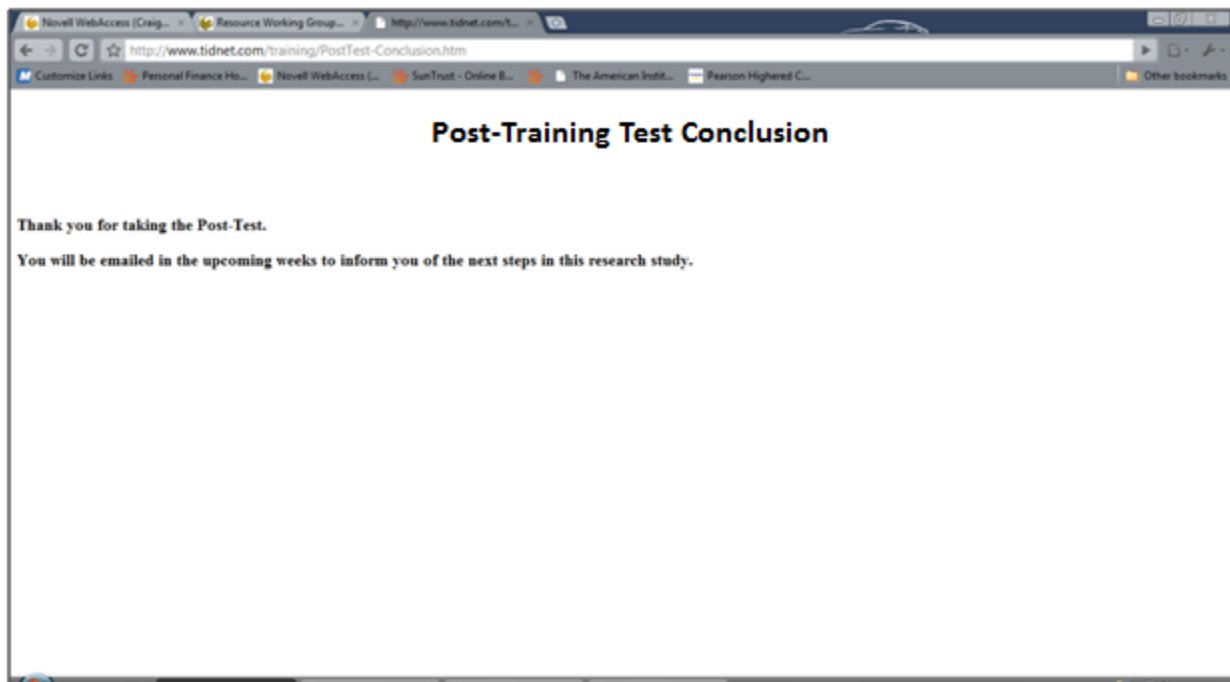


Figure 21 – Post-training Test Conclusion Screen

Three weeks after the completion of the post-training test, Groups A and B were sent an email directing them to the next phase of the training. This first follow-up training, as seen in Figure 22, reviewed some information that the subjects were exposed to in the initial security awareness training. After the subjects read the information on this first screen, they were sent to another screen (see Figure 23) that contained a bogus email simulation that attempted to extract confidential data from the subjects. If the subjects clicked on the fields to enter the data, a screen popped up with a warning that discussed the problems with replying to an email of this type, specifically that the Information Technology Department would not ask for this type of information. After they completed the simulated scenario, they were directed to a seven question test that checked their understanding and level of learning (see Figure 24). After the test, the subjects were sent to a conclusion screen (see Figure 25) thanking them for completing the first follow-up training with a simulated scenario and follow-up testing and informing them that they would again be contacted in the future for the next event.



Figure 22 - Follow Up Training - Week 3 Screen (page 1)

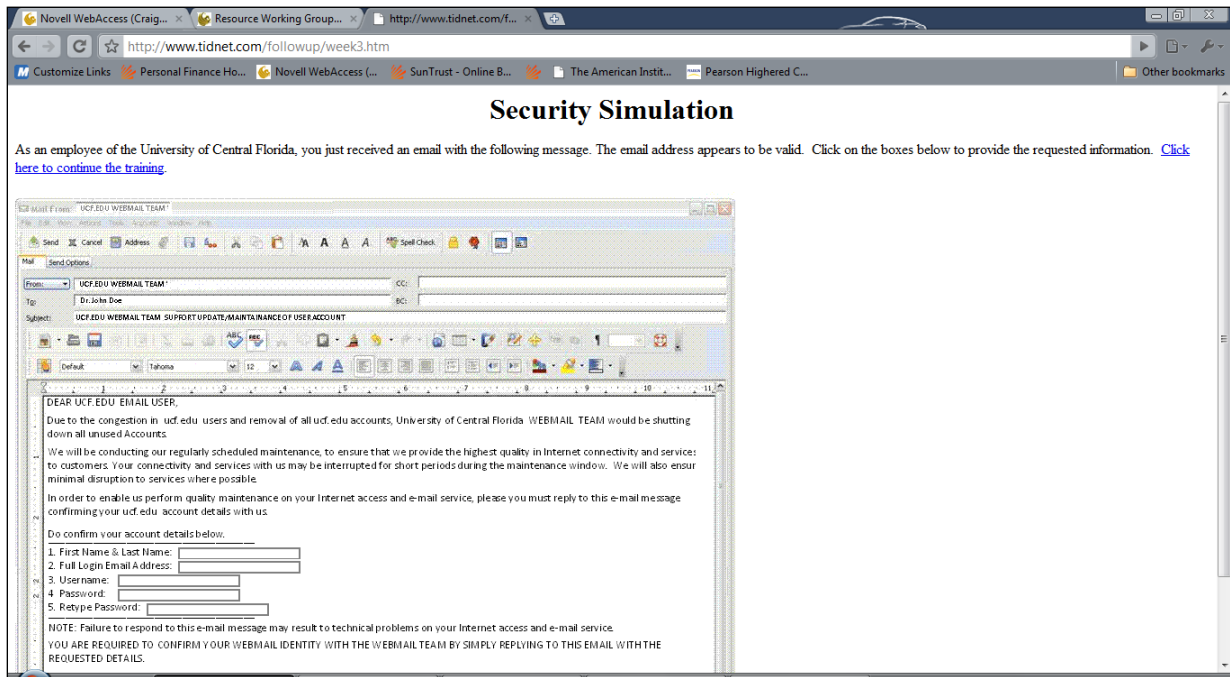


Figure 23 - Follow Up Training - Week 3 Simulation Screen

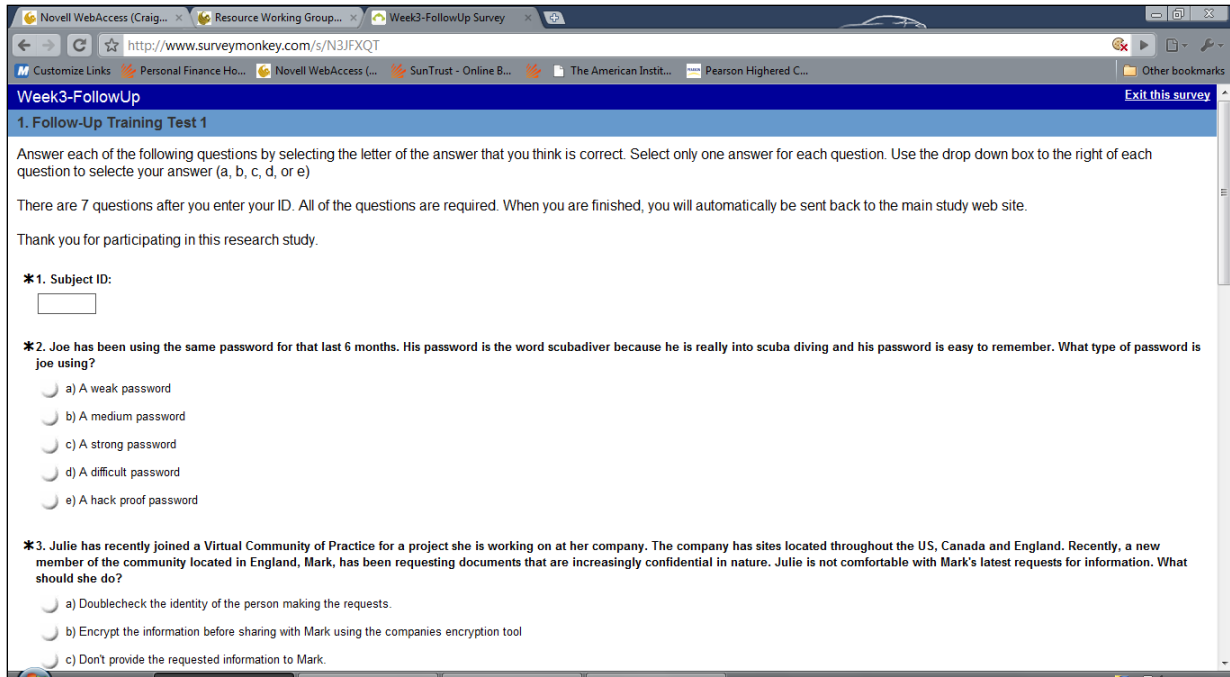


Figure 24 - Follow Up Training - Week 3 Test Screen

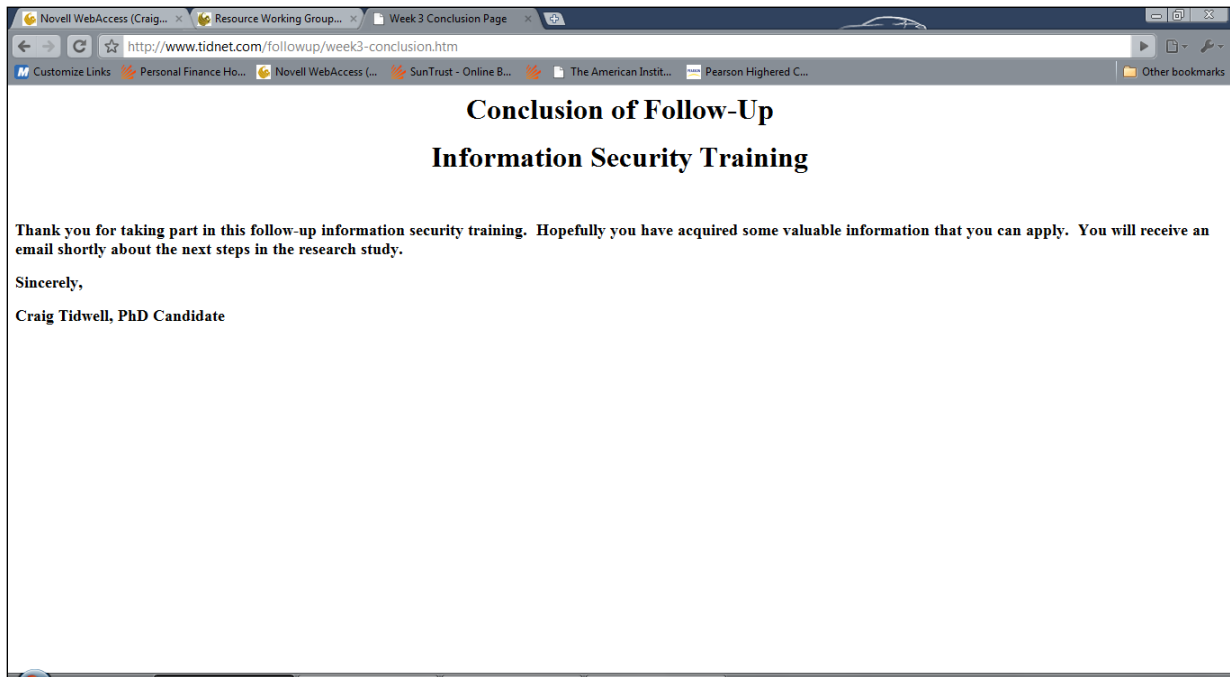


Figure 25 - Follow Up Training - Week 3 Conclusion Screen

Three weeks later, Groups A and B were sent an email with a link to the next follow-up information security awareness training with a simulated scenario and follow-up testing event (see Figure 26). This next event discussed the importance of having and enforcing a security policy and shared some examples of breaches that might result. Included on this page was another simulated scenario that checked the subjects' understanding of a phishing attempt (see Figure 27). Once again, the subjects were presented with an audio presentation that simulated a member of the Human Resources Department who claimed to need some information to process the subject's W2 form. Similar to the initial training with simulated scenarios scenario from the initial training event the subjects were asked to respond whether they should ("yes") or should not ("no") provide the information. If they selected "yes", they received a message that stated that they should not have provided the requested information. If they selected "no", they received a message praising them for their safe selection. After they completed the simulated scenario, they were taken to a seven question test that contained questions on information security (see Figure 28). After answering the questions, they were then thanked (see Figure 29) and informed of future upcoming events.

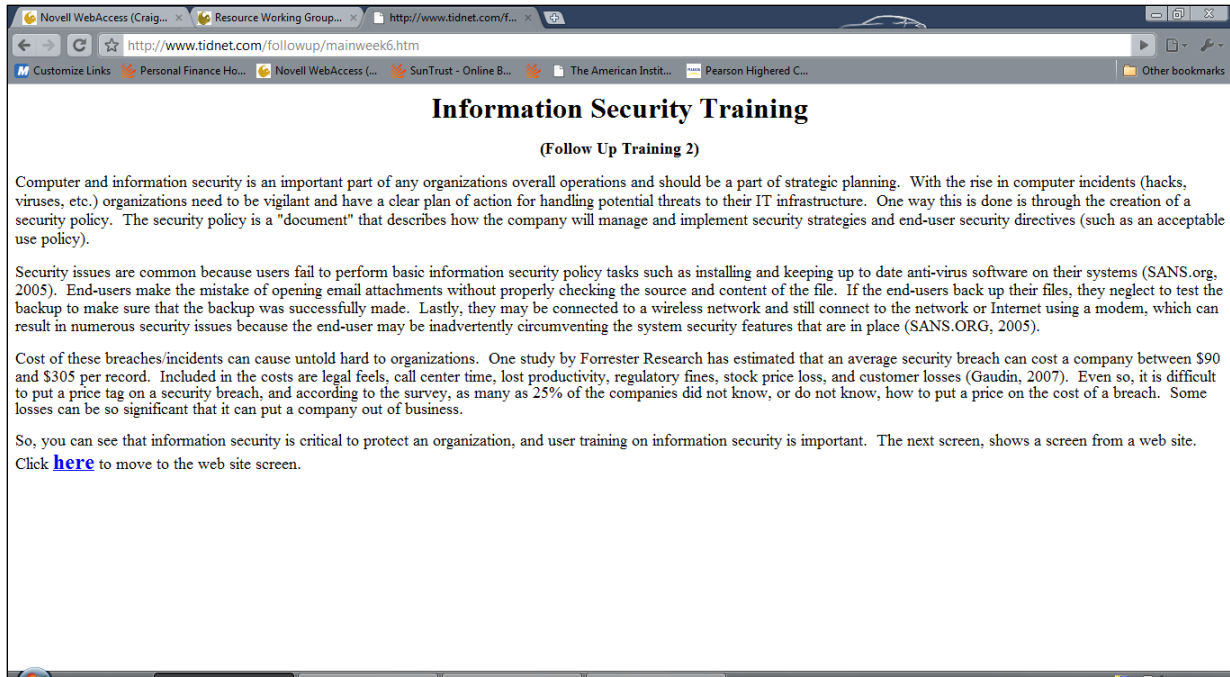


Figure 26 - Follow Up Training - Week 6 Screen (page 1)



Figure 27 - Follow Up Training - Week 6 Simulation Screen

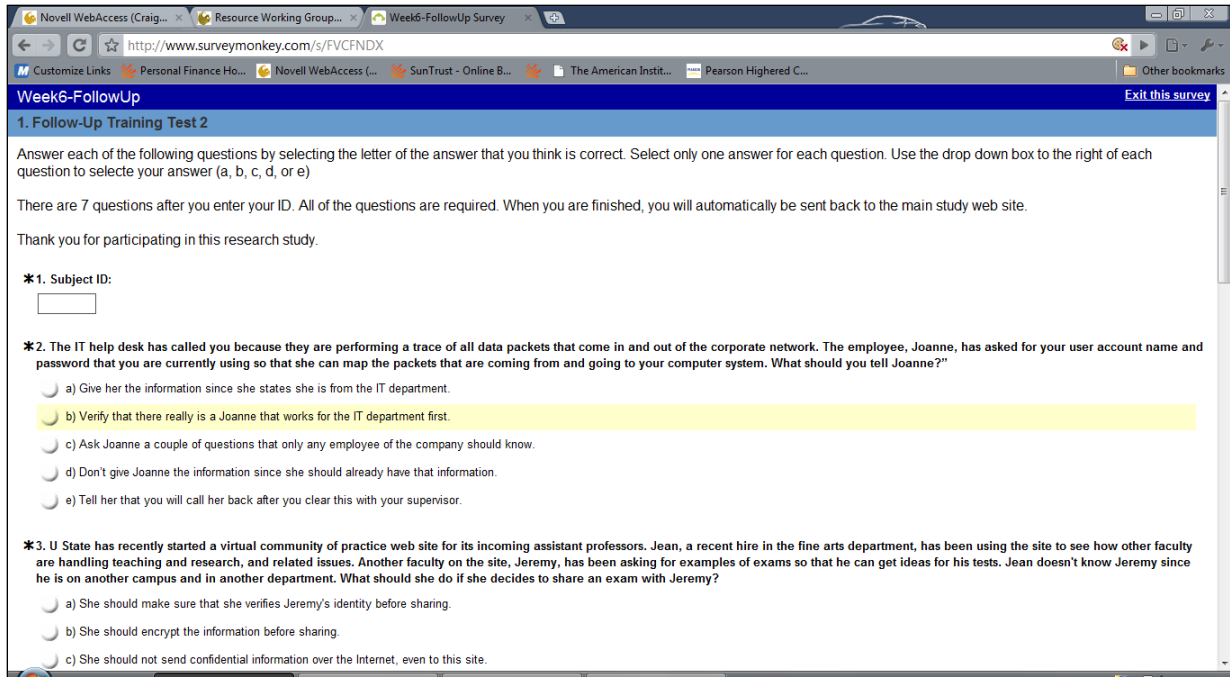


Figure 28 - Follow Up Training - Week 6 Test Screen

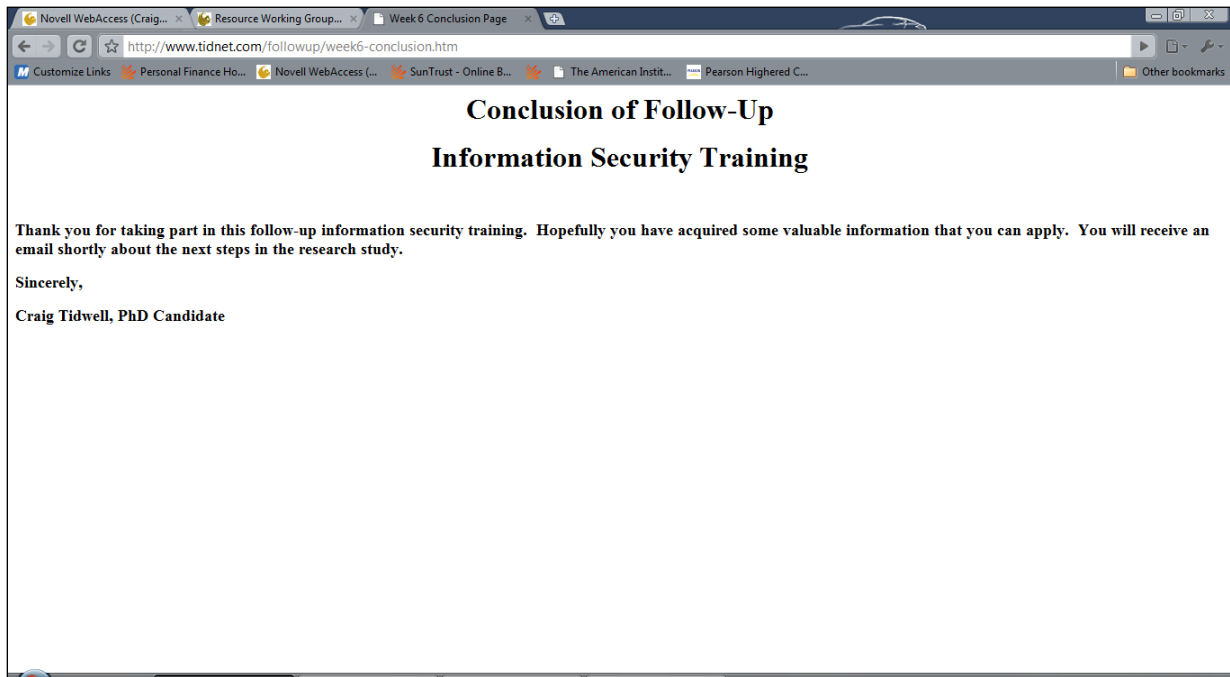


Figure 29 - Follow Up Training - Week 6 Conclusion Screen

The final follow-up training with a simulated scenario event was an email notice that was sent three weeks after the previous event. The email contained a link that directed the subjects from Groups A and B to the web page shown in Figure 30. Like the other follow-up training events, the page covered some information on information security and the risks of not following sound information security practices. After the subjects read the information on this screen they were directed to a simulated scenario (see Figure 31) which included a screen from a V-Cop. The subjects were asked to download a file from the simulated page of the V-Cop and if they attempted to do so, were presented with a warning pop-up screen explaining why they made a mistake. Once they completed the simulated scenario, they were taken to another seven-question test (see Figure 32) and then to a thank-you screen (see Figure 33).

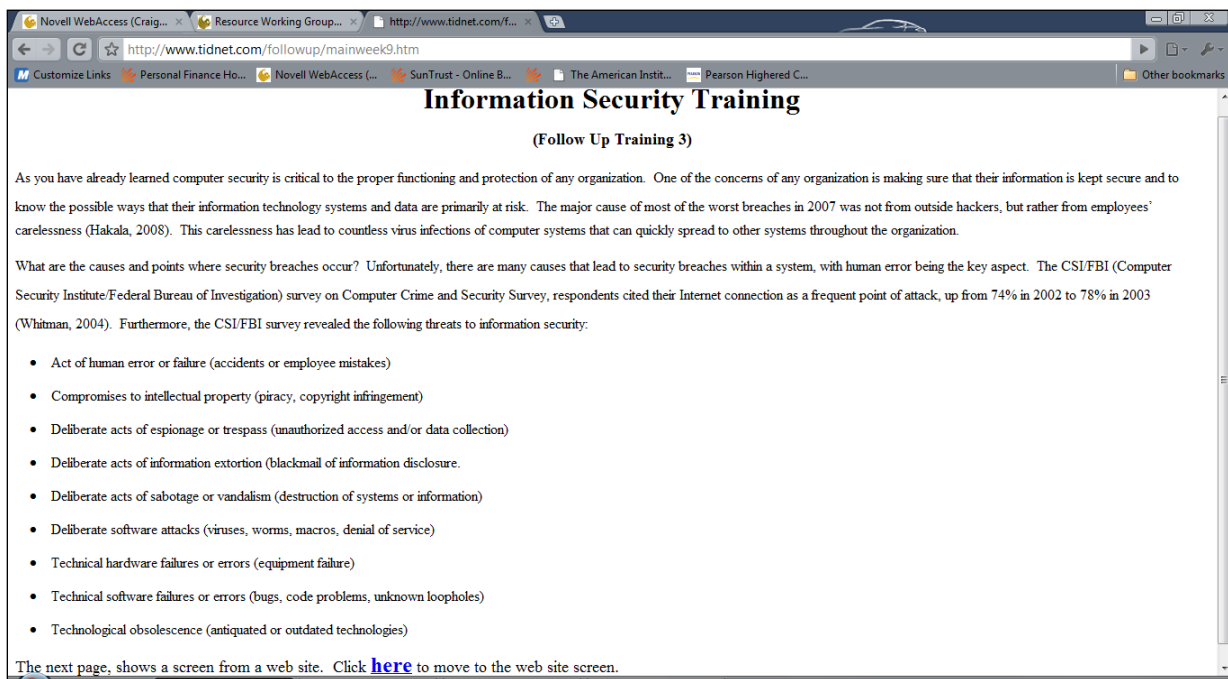


Figure 30 - Follow Up Training - Week 9 Screen (page 1)

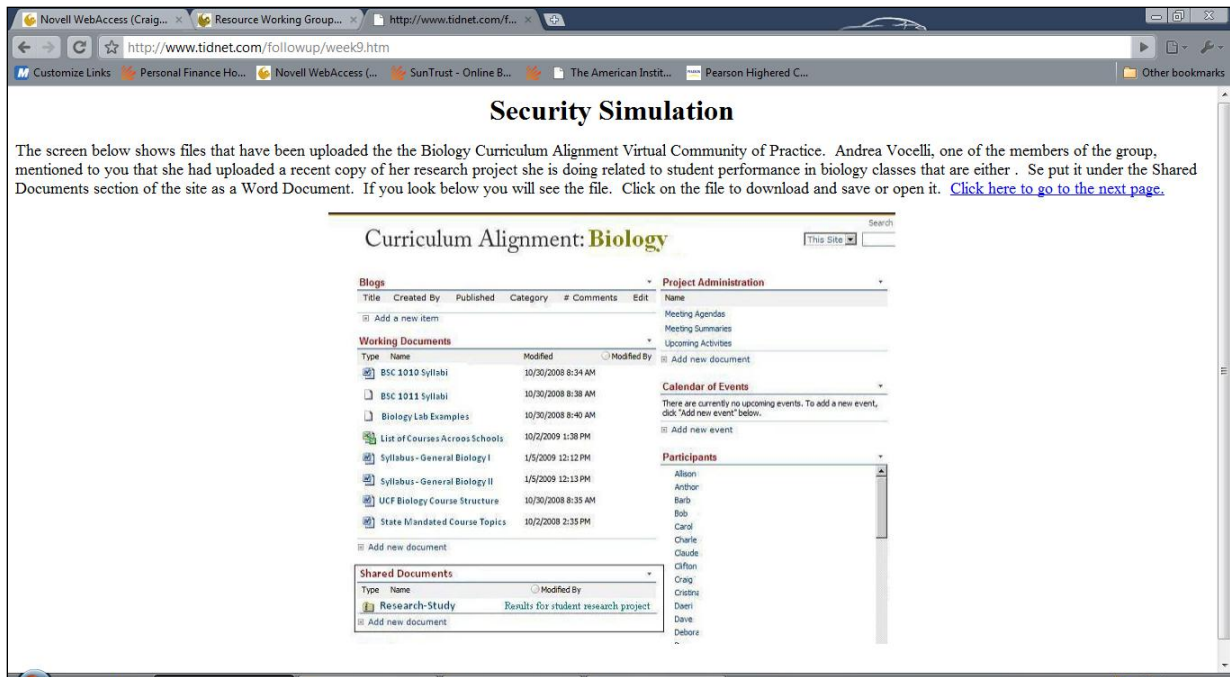


Figure 31 - Follow Up Training - Week 9 Simulation Screen

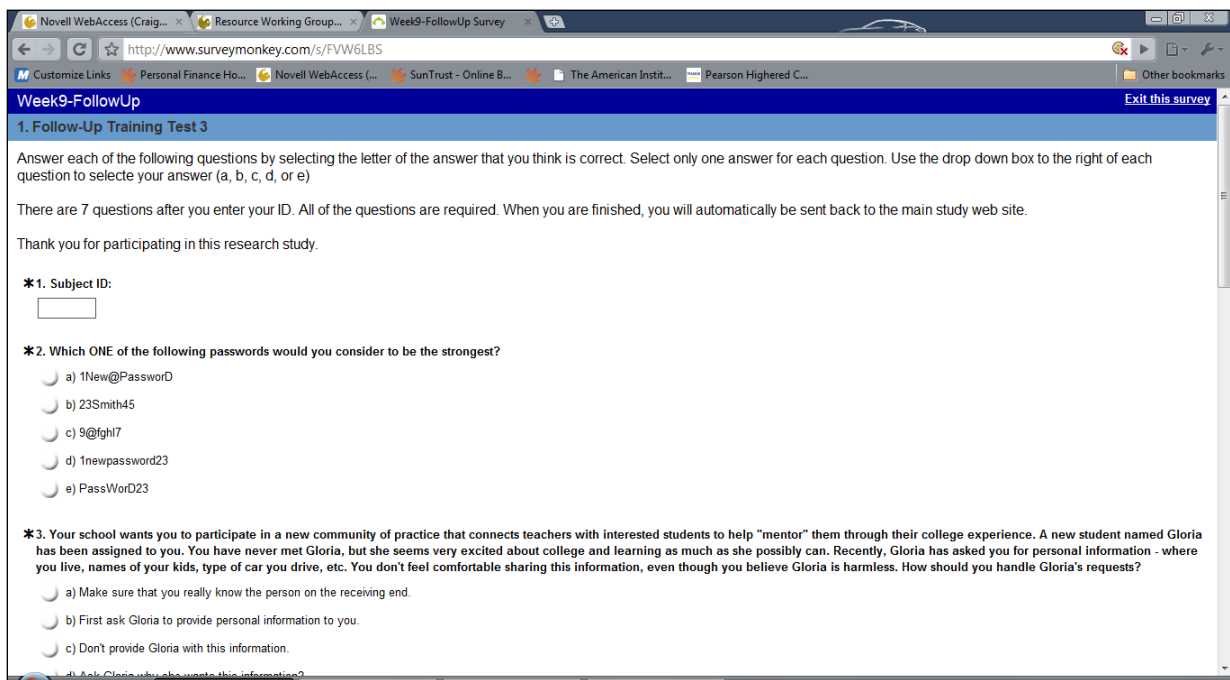


Figure 32 - Follow Up Training - Week 9 Test Screen

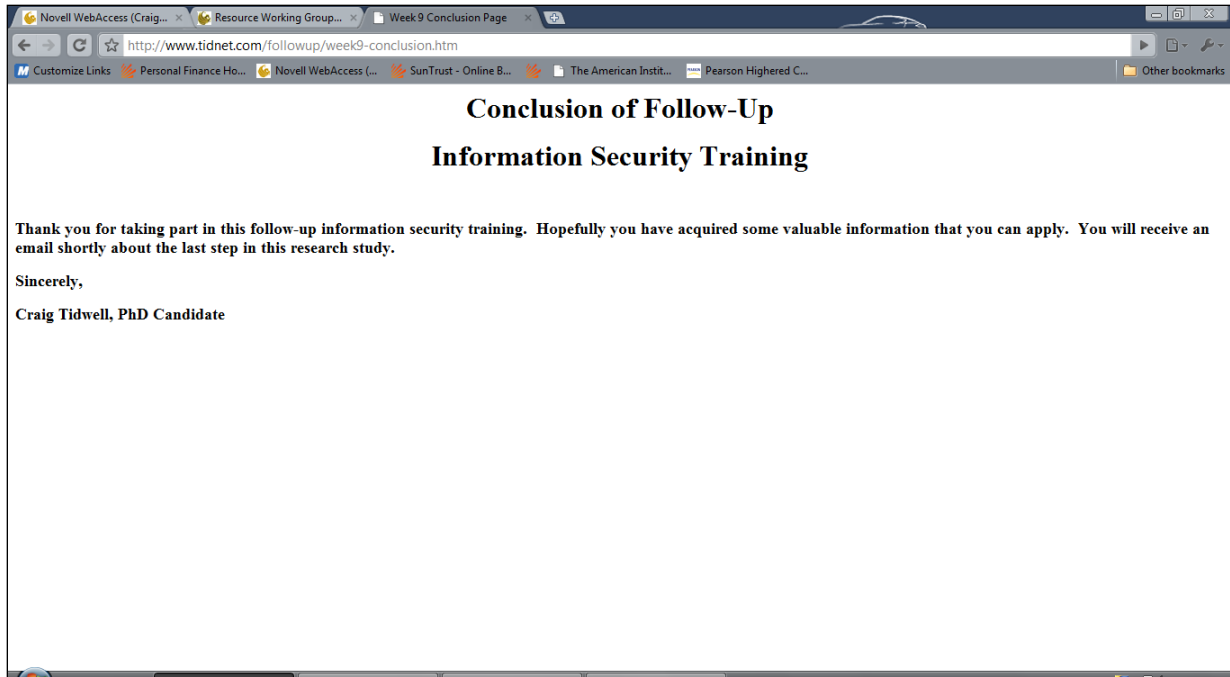


Figure 33 - Follow Up Training - Week 9 Conclusion Screen

One week after the third training event, Groups A, B, C, and D were sent an email that took them to the final test screen as seen in Figure 34. The screen had a link to the actual test which contained 20 questions that were identical to the pre-training test taken at the beginning of the research study (see Figure 35). Once they completed the final test, they were taken to a conclusion screen (see Figure 36) where they were thanked for their participation in the research study.

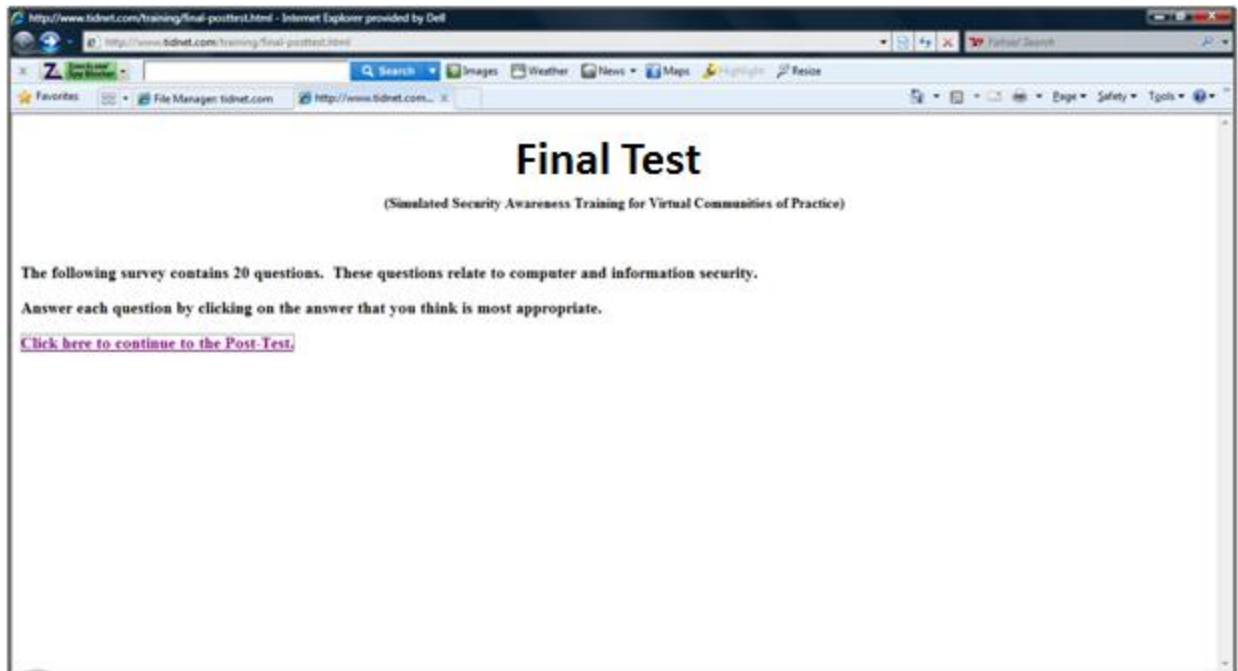


Figure 34 - Final Test Introduction Screen

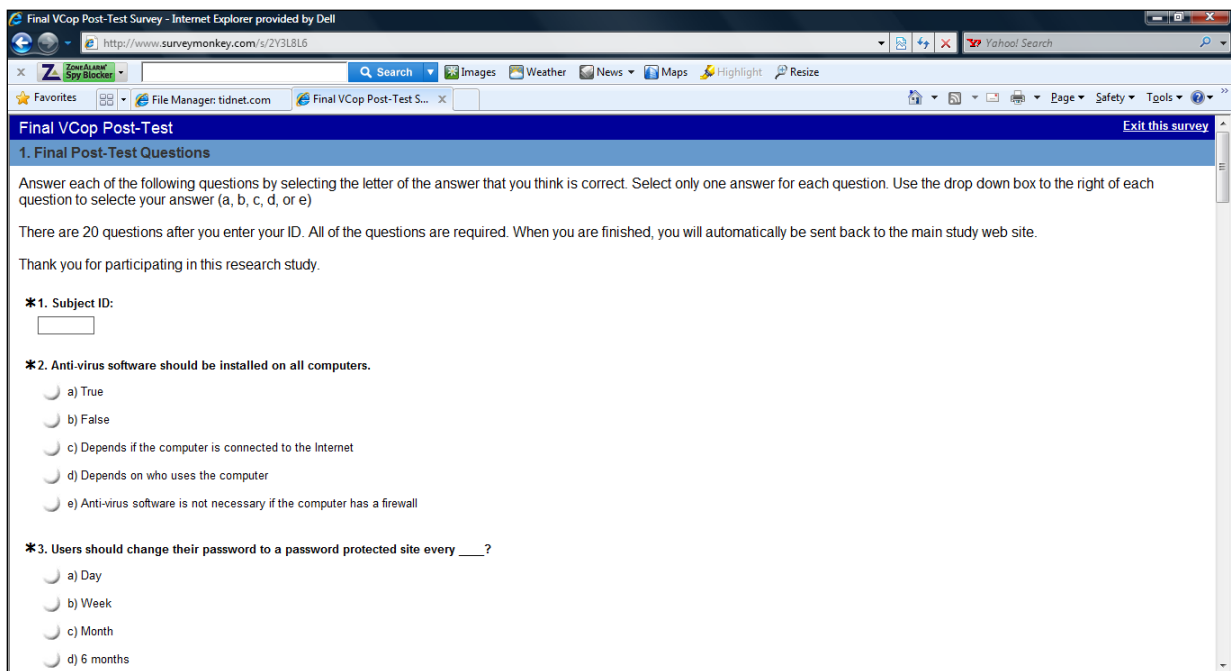


Figure 35 - Final Test Screen

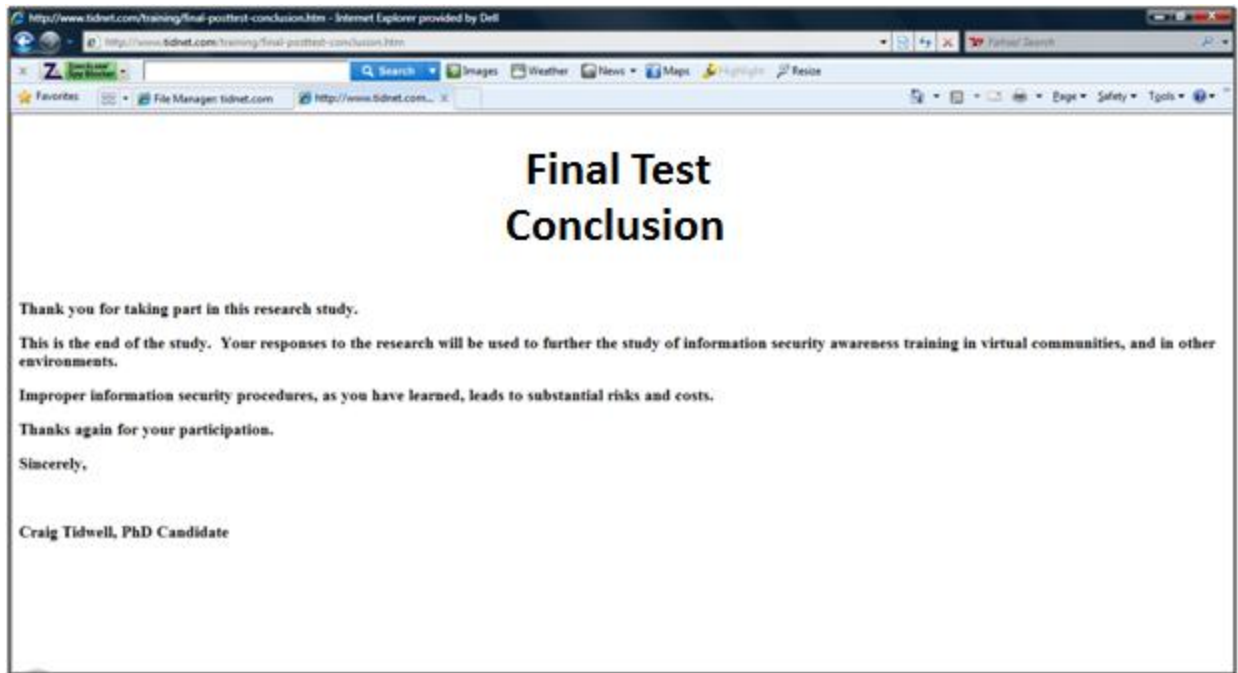


Figure 36 - Final Test Conclusion Screen

Analysis of Data

This section contains the data that was collected and the statistical results obtained from the research study. The mean, median, and standard deviation were computed for each subject across all questions and for each question across all subjects. Once the data was collected for a test, the Kruskal-Wallis test was used to determine if the corresponding null hypothesis should be accepted or rejected for tests with three or more groups.

The first set of data was collected from the pre-training test administered to Groups A, B, and C prior to any security training with simulated scenarios. The subjects were given a three-day window to take the pre-training test. Table 9 shows the summary results and Appendix C, Table 28, contains the collected scores for every subject and question for the pre-

training test. Each question had five multiple-choice answers, and the answers were ranked from 1 to 5, 1 for the least secure answer, and 5 for the most secure. The answers were ranked based on the literature review in Chapter 2, specifically from the information taken from the SANS web site (SANS.org, 2005).

Table 9 - Pre-training Test Summary Data

Subject ID	Mean	Median	Std Dev	Subject ID	Mean	Median	Std Dev	Subject ID	Mean	Median	Std Dev
A1	3.70	4.00	1.53	B1	3.55	4.00	1.36	C1	3.75	4.00	1.37
A2	4.35	5.00	1.04	B2	4.00	5.00	1.45	C2	3.65	4.00	1.18
A3	4.25	5.00	1.21	B3	3.45	3.00	1.61	C3	4.30	5.00	1.26
A4	4.30	5.00	1.13	B4	4.25	5.00	1.29	C4	3.90	5.00	1.48
A5	3.80	5.00	1.51	B5	4.25	5.00	1.02	C5	4.50	5.00	1.00
A6	3.80	4.50	1.47	B6	3.90	4.00	1.12	C6	4.15	5.00	1.18
A7	4.00	4.50	1.26	B7	4.35	5.00	1.18	C7	4.05	5.00	1.32
A8	3.85	4.50	1.39	B8	4.30	5.00	0.86	C8	3.40	3.50	1.47
Group A Average	4.01			Group B Average	4.01			Group C Average	3.96		

The mean scores over all the questions were identical for Groups A and B, and slightly lower for Group C. The questions that have lower than average results across all groups are questions 6, 18, and 20. These questions are located in Appendix B and the scores for these questions can be found in Table 28 in Appendix C. The average score across all groups was 2.26 for question 6, 2.72 for question 18, and 2.42 for question 20. Question 6 deals with data sharing, question 18 with passwords, and question 20 with the average cost of an information security breach. These three questions cover information security topics that were covered in the information security training that took place after the pre-training test that may require further focus. Question 20 is very specific and would require specific knowledge of the dollar cost of an information security breach which would not be commonly known. The other two questions also deal with issues that are not about basic information security awareness.

Even though the mean scores for these questions were lower than the other questions, the Kruskal Wallis rank-order testing revealed that there was no significance difference between the groups in the pre-training test. The results of the pre-training test suggest that the subject groups are very similar in their performance, making for more reliable data analysis that is not skewed by any of the subject groups. As the research progressed to the training with simulated scenarios, this similarity in scores provided a good foundation for data analysis.

Table 10 shows the results from the test using the Excel PhStat add-in at the 5% level of significance. The statistical test results were also computed manually. The results were identical as expected, providing assurance that the Kruskal-Wallis test was being performed properly. The pre-training test was not used to test a hypothesis, but to verify the similarity of the groups when looking at the post-training test and the final test.

Table 10 - Pre-training Test Kruskal Wallis Test Results

Pre-Test	
Data	
Level of Significance	0.05
Intermediate Calculations	
Sum of Squared Ranks/Sample Size	3760.563
Sum of Sample Sizes	24
Number of Groups	3
Test Result	
H Test Statistic	0.21125
Critical Value	5.991465
p-Value	0.899762
Do not reject the null hypothesis	

The next set of summary data shown in Table 11 comes from the post-training test which followed the initial training with simulated scenarios for Groups A and C and the pre-training test for Group B. The scores for each subject and question can be found in Table 28 located in Appendix C.

Table 11 - Post-training Test Summary Data

Subject ID	Mean	Median	Std Dev	Subject ID	Mean	Median	Std Dev	Subject ID	Mean	Median	Std Dev
A1	4.00	4.00	1.21	B1	3.70	4.00	1.26	C1	4.05	4.50	1.19
A2	4.30	5.00	1.17	B2	4.20	5.00	1.20	C2	4.05	4.50	1.32
A3	4.35	5.00	1.35	B3	3.60	4.00	1.47	C3	4.30	5.00	1.17
A4	4.45	5.00	1.05	B4	4.30	5.00	1.26	C4	4.00	5.00	1.30
A5	4.40	5.00	1.14	B5	4.15	4.50	0.99	C5	4.35	5.00	0.88
A6	4.20	5.00	1.36	B6	3.40	4.00	1.47	C6	4.20	5.00	1.20
A7	4.30	5.00	1.22	B7	4.25	5.00	1.16	C7	4.50	5.00	0.89
A8	4.05	5.00	1.43	B8	4.00	5.00	1.38	C8	4.20	5.00	1.28
Group A Average	4.26			Group B Average	3.95			Group C Average	4.21		

The post-training test responses were analyzed using standard summary statistics (see Table 29, Appendix C) and the Kruskal-Wallis test. The questions that showed the lowest overall average scores were numbers 4, 6, 17, and 18. Question 4 dealt with file sharing and shows a 1 point difference between Group B, which had a mean score of 2.63, and Group C, which had a mean score of 3.63. Since Group B did not receive the initial training with simulated scenarios, lower scores would have been expected. This may mean that more attention may need to be paid to file sharing in future security awareness training or simulated scenarios, or this difference could have been caused by a misunderstanding of the question and/or answers. The scores for question 6 were lower for all of the groups when compared to all of the other questions. Questions 17 and 18 have lower scores for Group B and covered material that may have been well known to the traditional user. Question 17 is about data

management, and question 18 is about password length. Since Group B did not receive the initial training, this may be the cause of these lower scores.

Table 12 shows the results of the Kruskal-Wallis test for the post-training test. Even though no significant difference was detected and the null hypothesis was not rejected, a difference did exist between Group B, a control group, and experimental Group A and control Group C. Both Groups A and C have higher mean scores and lower standard deviations.

Table 12 - Kruskal Wallis Post-Training Test Results at 5%

Post-Training Test	
Data	
Level of Significance	0.05
Intermediate Calculations	
Sum of Squared Ranks/Sample Size	3987
Sum of Sample Sizes	24
Number of Groups	3
Test Result	
H Test Statistic	4.74
Critical Value	5.991465
p-Value	0.093481
Do not reject the null hypothesis	

The p-value of 0.0934 for the post-training test reveals that for a higher level of significance such as 0.10, the results would have lead to reject the null hypothesis. Table 13 shows the Kruskal Wallis post-training test at 0.10. The training with simulated scenarios did make some difference from the pre- to the post-training test, even if that difference was not significant at the 5% level.

Table 13 - Kruskal Wallis Post-Training Test Results at 10%

Data	
Level of Significance	0.1
Intermediate Calculations	
Sum of Squared Ranks/Sample Size	3987
Sum of Sample Sizes	24
Number of Groups	3
Test Result	
H Test Statistic	4.74
Critical Value	4.60517
p-Value	0.093481
Reject the null hypothesis	

Table 14 shows the pre- and post-training test overall mean, median and standard deviation for Groups A, B and C. There was a positive change in the scores of Groups A and C after the training. Specifically, the mean scores increased for both Groups A and C by 0.25. This change, compared to Group B, is noticeable since Group B showed no change between the pre-training test and post-training test means.

Table 14 - Pre and Post-training Test Scores

Test	Group	Mean	Median	Std Dev	Group	Mean	Median	Std Dev	Group	Mean	Median	Std Dev
Pre-Training Test	A	4.01	5.00	1.32	B	3.95	5.00	1.27	C	3.96	5.00	1.31
Post-Training Test	A	4.26	5.00	1.56	B	3.95	4.00	1.51	C	4.21	5.00	1.15
Difference	A	0.25	0.00	0.24	B	0.00	-1.00	0.24	C	0.25	0.00	-0.16

The next set of collected data, Table 15, is from the first follow-up testing that took place approximately three weeks after the post-training test. Only Groups A and B received the follow-up training with a simulated event and testing.

Table 15 - Follow-Up Testing Data, Week 3

Subject ID	Questions									
Group A Received Training	1	2	3	4	5	6	7	Mean	Median	Std Dev
A1	a 5	c 5	a 5	b 5	d 5	c 5	d 5	5.00	5.00	0.00
A2	a 5	c 5	b 4	a 3	d 5	c 5	d 5	4.57	5.00	0.79
A3	a 5	c 5	a 5	b 5	d 5	c 5	e 3	4.71	5.00	0.76
A4	a 5	d 2	a 5	a 3	d 5	c 5	d 5	4.29	5.00	1.25
A5	a 5	c 5	b 4	a 3	d 5	c 5	a 2	4.14	5.00	1.21
A6	a 5	d 2	e 3	a 3	d 5	c 5	d 5	4.00	5.00	1.29
A7	a 5	d 2	a 5	b 5	d 5	c 5	d 5	4.57	5.00	1.13
A8	a 5	c 5	a 5	d 4	d 5	c 5	d 5	4.86	5.00	0.38
Mean	5.00	3.88	4.50	3.88	5.00	5.00	4.38	4.52		
Median	5.00	5.00	5.00	3.50	5.00	5.00	5.00			
Std Dev	0.00	1.55	0.76	0.99	0.00	0.00	1.19			
Subject ID	Questions									
Group B Received No Training	1	2	3	4	5	6	7	Mean	Median	Std Dev
B1	a 5	c 5	b 4	d 4	d 5	c 5	d 5	4.71	5.00	0.49
B2	a 5	e 1	a 5	b 5	c 4	c 5	a 2	3.86	5.00	1.68
B3	a 5	d 2	d 2	a 3	d 5	c 5	a 2	3.43	3.00	1.51
B4	a 5	e 1	b 4	b 5	d 5	c 5	d 5	4.29	5.00	1.50
B5	a 5	c 5	b 4	b 5	d 5	c 5	d 5	4.86	5.00	0.38
B6	a 5	d 2	b 4	b 5	d 5	d 4	d 5	4.29	5.00	1.11
B7	a 5	c 5	b 4	a 3	d 5	c 5	d 5	4.57	5.00	0.79
B8	a 5	a 4	b 4	d 4	d 5	c 5	d 5	4.57	5.00	0.53
Mean	5.00	3.13	3.88	4.25	4.88	4.88	4.25	4.32		
Median	5.00	3.00	4.00	4.50	5.00	5.00	5.00			
Std Dev	0.00	1.81	0.83	0.89	0.35	0.35	1.39			

With only two groups to compare, the Wilcoxon rank sum test was used. The overall mean score for both groups showed only a difference of 0.20. Also, examining the individual questions in the table, the differences between the lowest rank score and the highest rank score for the entire test was not as substantial as the pre- or post-training test. Overall, Group A did score higher on the test. The results of the Wilcoxon rank sum test are seen in Table 16. Even though Group A received the initial online simulated information security training, there was no significant difference at the 5% level of significance, so the null hypothesis was not rejected. Questions 2 and 3, which focus on phishing and social engineering, showed the biggest differences of 0.75 and 0.62. In both cases, Group A scored higher on the tests which may show that the initial training with simulated security scenarios had a greater impact.

Table 16 - Week 3 Follow-Up Test Results

Data	
Level of Significance	0.05
Population 1 Sample	
Sample Size	8
Sum of Ranks	75
Population 2 Sample	
Sample Size	8
Sum of Ranks	61
Intermediate Calculations	
Total Sample Size n	16
T1 Test Statistic	75
T1 Mean	68
Standard Error of T1	9.521904571
Z Test Statistic	0.735147044
Two-Tail Test	
Lower Critical Value	-1.959963985
Upper Critical Value	1.959963985
p-Value	0.462249946
Do not reject the null hypothesis	

Three weeks after the follow-up training for Week 3, another training with a simulated scenario and testing event was completed by Groups A and B. Table 17 shows the data from the Week 6 test. Even though Group A scored slightly higher than Group B, the gap narrowed when compared to the difference shown after the Week 3 follow-up test. The difference in the means was only 0.03, as compared to 0.20 from Week 3. The biggest difference in question scores occurred for question 4 which dealt with phishing. Group A had a higher score, with a difference of 0.87 for question 4. This may be a result of the initial training which had several sections that could be applied to this question.

Table 17 - Follow-Up Testing Data, Week 6

Subject ID:	Questions																
Group A	1		2		3		4		5		6		7		Mean	Median	Std Dev
A1	d	5	c	4	b	4	a	5	a	5	d	5	d	5	4.71	5.00	0.49
A2	e	4	c	4	d	3	a	5	b	4	b	4	d	5	4.14	4.00	0.69
a3	d	5	a	5	d	3	a	5	e	3	a	2	d	5	4.00	5.00	1.29
A4	d	5	c	5	d	3	a	5	e	3	a	2	d	5	4.00	5.00	1.29
A5	d	5	a	5	a	5	a	5	e	3	b	4	a	4	4.43	5.00	0.79
A6	d	5	a	5	d	3	c	3	a	5	b	4	d	5	4.29	5.00	0.95
A7	e	4	d	2	d	3	a	5	b	4	b	4	d	5	3.86	4.00	1.07
A8	d	5	d	2	d	3	a	5	a	5	d	5	d	5	4.29	5.00	1.25
Mean		4.75		4.00		3.38		4.75		4.00		3.75		4.88	4.21		
Median		5.00		4.50		3.00		5.00		4.00		4.00		5.00			
Std Dev		0.46		1.31		0.74		0.71		0.93		1.16		0.35			
Group B															Mean	Median	Std Dev
B1	d	5	c	4	d	3	d	4	b	4	c	3	d	5	4.00	4.00	0.82
B2	d	5	c	4	b	4	c	3	a	5	d	5	d	5	4.43	5.00	0.79
B3	d	5	d	2	d	3	d	4	d	2	d	5	a	4	3.57	4.00	1.27
B4	d	5	a	5	a	5	b	2	b	4	a	2	d	5	4.00	5.00	1.41
B5	d	5	c	4	a	5	a	5	b	4	d	5	d	5	4.71	5.00	0.49
B6	d	5	c	4	d	3	c	3	e	3	d	5	d	5	4.00	4.00	1.00
B7	b	3	a	5	a	5	a	5	b	4	d	5	d	5	4.57	5.00	0.79
B8	d	5	d	2	d	3	a	5	b	4	d	5	d	5	4.14	5.00	1.21
Mean		4.75		3.75		3.88		3.88		3.75		4.38		4.88	4.18		
Median		5.00		4.00		3.50		4.00		4.00		5.00		5.00			
Std Dev		0.71		1.16		0.99		1.13		0.89		1.19		0.35			

The Wilcoxon Rank sum test was again used to analyze the test results data and to determine if there was a significant difference between the two groups. Table 18 shows that there was not a significant difference so the null hypothesis was not rejected and we reject the second research hypothesis that there was a significant difference between the groups after the Week 6 online training with a simulated scenario, and testing event on information security.

Table 18 - Week 6 Follow-Up Test Results

Data	
Level of Significance	0.05
Population 1 Sample	
Sample Size	8
Sum of Ranks	69.5
Population 2 Sample	
Sample Size	8
Sum of Ranks	66.5
Intermediate Calculations	
Total Sample Size n	16
T1 Test Statistic	69.5
T1 Mean	68
Standard Error of T1	9.521905
Z Test Statistic	0.157532
Two-Tail Test	
Lower Critical Value	-1.95996
Upper Critical Value	1.959964
p-Value	0.874826
Do not reject the null hypothesis	

However, when we compare the results from the Week 3 and Week 6 training with simulated scenario and follow-up testing, we do see a slight difference as shown in Table 19. But the difference is slightly negative for both Groups A and B, since their average scores dropped between the two tests. This could be in part due to the differences in the training and testing event or it could be attributable to the length of time between the initial training with simulated scenarios and the follow-up testing results.

Table 19 - Week 3 and Week 6 Test Results

	Group	Mean	Median	Std Dev	Group	Mean	Median	Std Dev
Week 3	A	4.52	5.00	0.99	B	4.32	5.00	1.13
Week 6	A	4.22	5.00	0.99	B	4.18	5.00	1.01

Three weeks after the Week 6 test, the final follow-up training with a simulated scenario and testing event took place. Groups A and B completed the training and testing. Table 20 shows the data that was collected from the Week 9 testing. The mean score changed slightly between the 2 groups from 0.03 from Week 6 to 0.40 for Week 9, the largest difference computed for all three training with

simulated scenarios and testing events. The biggest difference in scores occurred for question 7. Group A had a mean score of 4.25 and Group B had a mean score of 3.25 for the question which deals with phishing. There seems to be a common thread for Week 3, 6, and 9 testing. Perhaps further training and testing is needed for phishing and social engineering. However, even though this difference exists, the scores are still strong across the test with an overall mean of 4.63 for Group A and 4.23 for Group B.

Table 20 - Follow-Up Testing Data, Week 9

Subject ID	Questions												Mean	Median	Std Dev		
	1	2	3	4	5	6	7	8	9	10	11	12					
A1	a	5	c	5	d	4	c	5	e	2	d	5	b	3	4.14	5.00	1.21
A2	c	4	c	5	a	5	a	4	d	5	d	5	d	5	4.71	5.00	0.49
A3	c	4	c	5	a	5	c	5	d	5	d	5	d	5	4.86	5.00	0.38
A4	c	4	c	5	a	5	c	5	d	5	d	5	d	5	4.86	5.00	0.38
A5	a	5	c	5	a	5	c	5	d	5	a	3	d	5	4.71	5.00	0.76
A6	c	4	c	5	a	5	a	4	d	5	d	5	d	5	4.71	5.00	0.49
A7	c	4	c	5	d	4	c	5	d	5	d	5	d	5	4.71	5.00	0.49
A8	c	4	c	5	a	5	c	5	d	5	d	5	e	1	4.29	5.00	1.50
Mean		4.25		5.00		4.75		4.75		4.63		4.75		4.25	4.63		
Median		4.00		5.00		5.00		5.00		5.00		5.00		5.00			
Std Dev		0.46		0.00		0.46		0.46		1.06		0.71		1.49			
															Mean	Median	Std Dev
B1	d	1	c	5	d	4	c	5	d	5	d	5	c	2	3.86	5.00	1.68
B2	a	5	c	5	b	2	c	5	d	5	e	2	b	3	3.86	5.00	1.46
B3	b	2	a	3	a	5	b	3	d	5	a	3	c	2	3.29	3.00	1.25
B4	c	4	c	5	a	5	c	5	d	5	d	5	b	3	4.57	5.00	0.79
B5	c	4	c	5	a	5	c	5	d	5	d	5	e	1	4.29	5.00	1.50
B6	a	5	c	5	c	3	a	4	d	5	d	5	d	5	4.57	5.00	0.79
B7	c	4	c	5	a	5	c	5	d	5	d	5	d	5	4.86	5.00	0.38
B8	c	4	d	4	d	4	c	5	d	5	d	5	d	5	4.57	5.00	0.53
Mean		3.63		4.63		4.13		4.63		5.00		4.38		3.25	4.23		
Median		4.00		5.00		4.50		5.00		5.00		5.00		3.00			
Std Dev		1.41		0.74		1.13		0.74		0.00		1.19		1.58			

The Wilcoxon rank sum test was used to compare the results for Groups A and B on the Week 9 follow-up test. Table 21 indicates that the data did not show a significant difference between the groups, so the null hypothesis was not rejected and the second research question is not confirmed. The p-value was relatively low so running the test at a 7% level of significance would have produced a different conclusion and the null hypothesis would have been rejected.

Table 21 - Week 9 Follow-Up Test Results

Data	
Level of Significance	0.05
Population 1 Sample	
Sample Size	8
Sum of Ranks	85.5
Population 2 Sample	
Sample Size	8
Sum of Ranks	50.5
Intermediate Calculations	
Total Sample Size n	16
T1 Test Statistic	85.5
T1 Mean	68
Standard Error of T1	9.521904571
Z Test Statistic	1.83786761
Two-Tail Test	
Lower Critical Value	-1.959963985
Upper Critical Value	1.959963985
p-Value	0.066081916
Do not reject the null hypothesis	

The complete follow-up training and testing results are summarized in Table 22 which shows the summary data statistics across all three tests.

Table 22 - Week 3, 6, and 9 Summary Data Statistics

	Group	Mean	Median	Std Dev	Group	Mean	Median	Std Dev
Week 3	A	4.52	5.00	0.99	B	4.32	5.00	1.13
Week 6	A	4.22	5.00	0.99	B	4.18	5.00	1.01
Week 9	A	4.63	5.00	0.99	B	4.23	5.00	1.18

We see from this table that the changes in the mean, median and standard deviation of the scores were minimal, with a slight drop and then rise for Group A. The same trend occurred for Group B. Group A did recover to a higher level than Group B at the conclusion of the Week 9 training with simulated scenarios and testing event. The standard deviation stayed the same for Group A and changed slightly for Group B. At first glance this seems to indicate that the training and testing had no

effect on the subjects. However, another possible way to look at these results may be to show the consistency of scores for Group A. The subjects were consistent across the three events. Since Group A, the experimental group, maintained the higher score values throughout the testing, it may be concluded that the initial training with simulated scenarios did make some positive difference.

The data from the final test is presented last. The final test was taken by all four groups. Group D completed the demographic survey and took the final test, and was used as one of the control groups to determine the effect that may be caused by partial training and testing. The final test contained the exact same questions as the pre-training test to ensure that the same data was being tested. There was a time span of about twelve weeks between the pre-training test and the final test. Table 23 shows the summary data from the final test. The complete listing of scores for each subject and for each question can be found in Appendix C, Table 30. The results did not show a significant difference between the groups, even for Group D who did not receive any previous testing or training.

Table 23 - Final Test Summary Results

Subject			Std	Subject			Std
ID	Mean	Median	Dev	ID	Mean	Median	Dev
A1	3.55	4.00	1.24	B1	3.75	4.00	1.41
A2	4.35	5.00	1.14	B2	4.20	5.00	1.28
A3	4.00	5.00	1.41	B3	3.55	4.00	1.64
A4	4.30	5.00	1.13	B4	4.00	4.50	1.21
A5	3.65	4.50	1.53	B5	4.40	5.00	0.99
A6	4.30	5.00	1.22	B6	3.75	4.00	1.29
A7	4.05	5.00	1.32	B7	4.35	5.00	1.18
A8	4.00	5.00	1.41	B8	4.35	5.00	0.81
Group	4.03	5.00	1.30	Group	4.04	5.00	1.26
Subject			Std	Subject			Std
ID	Mean	Median	Dev	ID	Mean	Median	Dev
C1	3.90	4.50	1.37	D1	4.00	5.00	1.41
C2	3.95	4.00	1.15	D2	3.65	4.50	1.60
C3	4.15	5.00	1.35	D3	3.90	5.00	1.62
C4	3.75	5.00	1.52	D4	4.35	5.00	1.23
C5	4.40	5.00	0.99	D5	4.25	5.00	0.97
C6	4.25	5.00	1.16	D6	4.05	5.00	1.28
C7	3.95	5.00	1.32	D7	3.75	4.00	1.37
C8	3.50	4.00	1.50	D8	3.95	5.00	1.32
Group	3.98	5.00	1.31	Group	3.99	5.00	1.35

The final analysis of the data using the Kruskal-Wallis test did not show a significant difference at the 5% level so the null hypothesis was not rejected. The third research hypothesis is not confirmed, which implies that there was no significant difference between the groups' mean scores. Table 24 shows the results of the Kruskal-Wallis test. The p-value is almost equal to 1.0 which further confirmed the results.

Table 24 - Final Test Results

Kruskal-Wallis Final Post-Test	
Data	
Level of Significance	0.05
Intermediate Calculations	
Sum of Squared Ranks/Sample Size	8761.813
Sum of Sample Sizes	32
Number of Groups	4
Test Result	
H Test Statistic	0.566051
Critical Value	7.814728
p-Value	0.904158
Do not reject the null hypothesis	

Table 25 shows the final results of all the groups for the final test and Groups A, B, and C on the pre-training test, post-training test, and the final test at the end of the research study. It is interesting to note that the scores on the pre-training test were almost identical to the final test which was composed of the exact same questions. This lack of improvement from the experimental group could be attributable to a number of reasons. Perhaps the subjects thought too much about the answers or did not spend an adequate amount of time on the final test and rushed through the questions. What is most fascinating is the lack of significant difference between the experimental Group A and control Group D who had received no security testing or training before taking the final test. The means for Groups A and D differ by only 0.04 (Group A had a mean of 4.03 and Group D 3.99). Perhaps the level of knowledge of Group D exceeded that of the other groups, or perhaps the training with simulated scenarios and testing did not impact the subjects as hypothesized. However, even though the scores of

the groups did not increase significantly, they also did not decrease which would lead one to believe that the training with simulated scenarios and follow-up testing at least kept the scores from dropping over time. Further examination and research is warranted as explained in Chapter 5.

Table 25 - Final Comparison of Groups

Test	Group	Mean	Median	Std Dev	Group	Mean	Median	Std Dev	Group	Mean	Median	Std Dev	Group	Mean	Median	Std Dev
Pre-Training Test	A	4.01	5.00	1.32	B	3.95	5.00	1.27	C	3.96	5.00	1.31				
Post-Training Test	A	4.26	5.00	1.56	B	3.95	4.00	1.51	C	4.21	5.00	1.15				
Week 3 Follow-Up	A	4.52	5.00	0.99	B	4.32	5.00	1.13								
Week 6 Follow-Up	A	4.22	5.00	0.99	B	4.18	5.00	1.01								
Week 9 Follow-Up	A	4.63	5.00	0.99	B	4.23	5.00	1.18								
Final Test	A	4.03	5.00	1.30	B	4.04	5.00	1.26	C	3.98	5.00	1.31	D	3.99	5.00	1.35

CHAPTER FIVE: FINDINGS, CONCLUSIONS, AND FUTURE RESEARCH

Recap of the Study

The purpose of the research study was to examine the effects of information security awareness training with simulated scenarios and follow-up testing on members of a V-CoP. The literature revealed a general lack of security awareness training but, through proper security controls accompanied by security awareness education, this trend can be diminished (Whitman, 2004). The research questions asked if the security awareness training with simulated scenarios and follow-up testing would improve the scores on information security tests, specifically after repeated training and testing were done over an approximately twelve-week time period. The underlying assumption was that scores on information security tests are directly related to information security awareness and conformance. Deterrence theory was used as the grounded theory as subjects were educated on the security threats and their negative impact and consequences throughout the training and simulated scenarios.

The community that was used for this research consisted of faculty members that are part of a V-CoP for curriculum alignment with the University of Central Florida's Regional Campuses and were equally distributed among the four research groups. The data was collected in the following order: demographic data was collected for all 32 subjects (see Appendix A); Groups A, B, and C took a pre-training test to assess their initial knowledge of information security awareness (see Appendix B); Groups A and C completed the initial

simulated security training (see Chapter 4); Groups A, B, and C then completed a post-training test after the initial training made up of questions very similar to the pre-training test questions; Groups A and C then participated in follow-up training with simulated scenarios and testing events at 3 weeks, 6 weeks, and 9 weeks after the post-training test taken after the initial training with simulated scenarios; the last event was the final test which was taken by all of the groups approximately one week after the Week 9 follow-up training and testing event. The training events and tests were created from the information presented in the Chapter 2 literature review. The test questions were created based on the information gleaned from the SANS Institute (SANS.org, 2009), the new information security taxonomy by Kjaerland (Kjaerland, 2006; CERT/CC, 2004), and the 2003 CSI/FBI survey on Computer Crime and Security Survey (Whitman, 2004).

Findings

From the data presented in Chapter 4, and the preliminary analysis of that data, it was determined that the security awareness training with simulated security scenarios and follow-up testing did not produce enough of an improvement in the information security awareness test scores to reject all of the null hypotheses at the 5% level of significance. However, between the pre- and post-training test the null hypotheses would have been rejected at the 10% level of significance. The statistical power of the tests is low as the number of subjects was relatively small in each group. Nevertheless, the Kruskal-Wallis test procedure is approximately valid since the sample groups all contain more than five subjects (observations).

Some of the implications from the findings could be that the training may not be useful for long term change in security awareness for members of a V-CoP. It may also mean that the simulated scenarios were not effective and may not be necessary for security awareness training. The use of deterrence theory may not be as effective as using a theory that does not focus on the detrimental effects of information security breaches. A less educated and experienced target group may provide for different results than the group used for this study as shown by their initially high test scores. Lastly, this type of training with simulated scenarios may not be effective on more educated V-CoP members and other methods or levels of training may be more effective. Either way, further research is needed.

A graphic representation of the data found in Table 25 is shown in Figure 37. The chart shows the overall scores for Group A, the experimental group, and any changes in test results for control Groups B, C, and D. Group A did show an increase in results from the pre-training test until the drop in the mean score at the Week-6 test, and then the mean test score increased at the Week-9 test and then, after completing the final test, returned to almost the identical scores as the pre-training test. Group D, who received no simulated information security awareness training, scored at almost the same level as Group A, who received all of the information security awareness training and testing. The questions in the pre-training test and the final test were identical except for randomization of the answer choices. Group B did not receive the initial simulated information security awareness training and showed an upward trend in performance between the post-training test and Week 3 follow-up test.

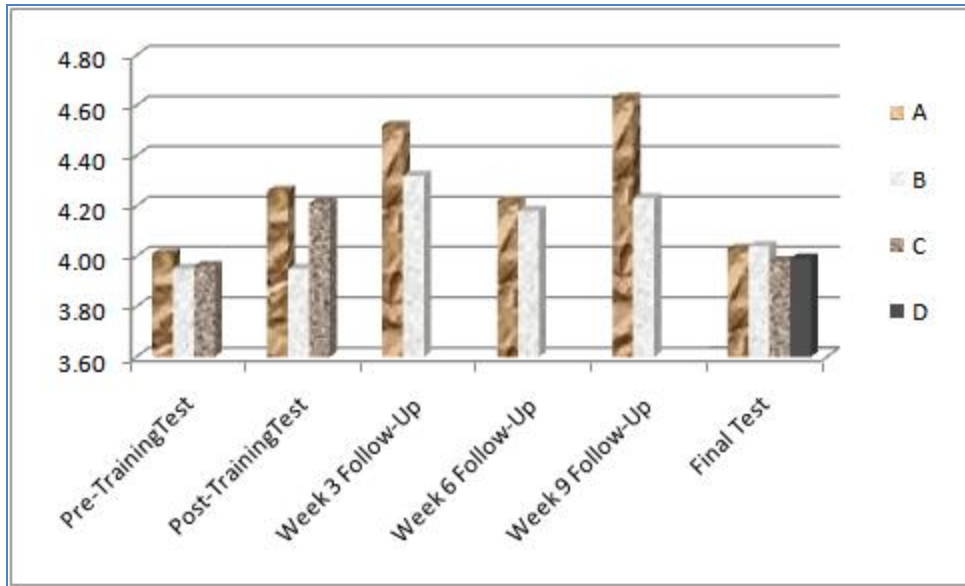


Figure 37 - Bar Chart of Test Score Data

Confidence intervals were calculated at the 95% confidence level for each group for each test that they completed (see Table 26). Confidence intervals were also computed for each test for all of the groups (see Table 31 in Appendix G). The confidence intervals are relatively wide since the sample sizes are modest. It is therefore not surprising that the tests of hypotheses showed no statistically significant difference at the 5% significance level.

Table 26 – Confidence Intervals at 95%

Test and Group	Lower Limit	Upper Limit
Pre-Training Test for Group A	3.095	4.925
Pre-Training Test for Group B	3.070	4.830
Pre-Training Test for Group C	3.102	4.918
Pre-Training Test for Groups A, B, C	3.470	4.510
Post-Training Test for Group A	3.179	5.000
Post-Training Test for Group B	2.904	4.996
Post-Training Test for Group C	3.413	5.000
Post-Training Test for Group A, B, C	3.648	4.632
Final Test for Group A	3.129	4.931
Final Test for Group B	3.167	4.913
Final Test for Group C	3.072	4.888
Final Test for Group D	3.055	4.925
Final Test for Group A, B, C, D	3.570	4.470
Week3 Follow-Up A	3.834	5.000
Week3 Follow-Up B	3.537	5.000
Week3 Follow-Up A, B	3.906	4.934
Week6 Follow-Up A	3.534	4.906
Week6 Follow-Up B	3.480	4.880
Week6 Follow-Up A, B	3.715	4.685
Week9 Follow-Up A	3.944	5.000
Week9 Follow-Up B	3.412	5.000
Week9 Follow-Up A, B	3.612	5.000

The following three figures show the test score trend lines for Groups A, B, and C. The trend lines show the mean scores for each test taken by the specified group. The pre-training test, post-training test, and final test contained 20 questions, and the Week 3, Week 6 and Week 9 tests contained 7 questions each (see Appendix B). The scores for Groups A and B dipped slightly at Week 6, and then improved slightly at Week 9. But, even with these slight changes in results between the various tests and groups, the overall changes show that no significant changes occurred between the experimental group and the control groups at the 0.05 level. The exception to this was when the level of significance for the post-training test was changed to 0.10, at which time the null hypothesis was rejected that there was no difference between the scores of the groups. Group A and Group C did show an improvement in

their mean scores of 0.25 on a 5 point scale. Even though at the 0.05 level there was no significant difference between the groups' means, there was also no decrease in performance of Group A with even a slight increase between the pre-training test and final test as shown in Figure 38. There was an increase in test performance for the Groups A and B who received the initial training with simulated scenarios. This seems to show that the training was at least temporarily effective in improving information security awareness.

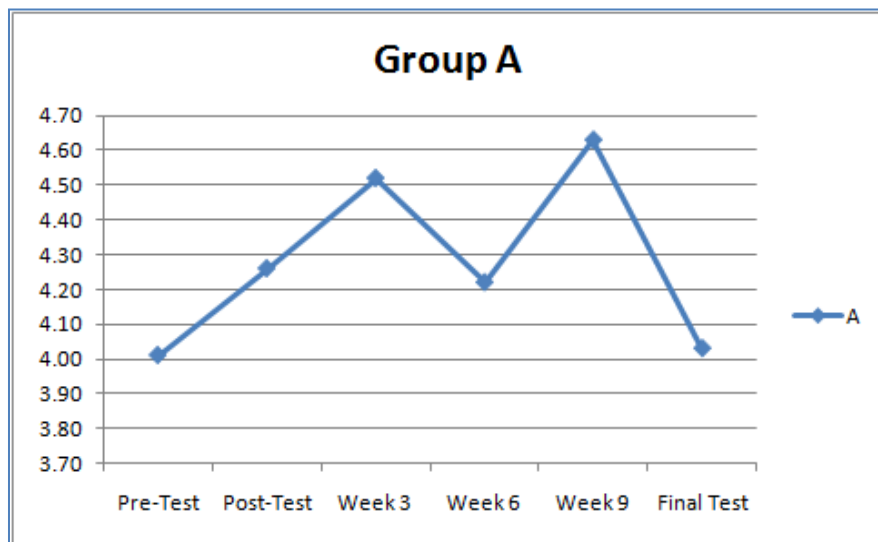


Figure 38 - Line Graph of Group A Data

Group B did not receive the initial information security simulated awareness training and pre-training testing which would explain the identical scores recorded for Group B for the pre-training test and post-training test. After Group A and B received the follow-up Week 3 training, their test scores increased and stayed higher, even though the increase was not significant enough to reject the null hypothesis. However, between Group A and Group B, there was an initial improvement in scores after the Week-3 training. Group B's scores remained flat between the pre-training information security

awareness test and the post-training test, while A showed an increase between the initial pre-training test and post-training test following the training (as previously discussed).

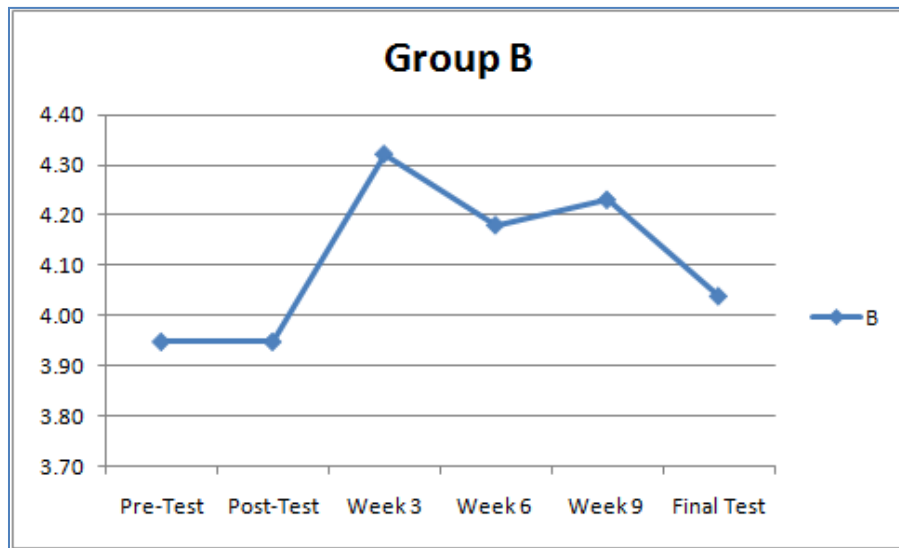


Figure 39 - Line Graph of Group B Data

Group C received the initial training and testing, but no follow up training and testing. There was a difference in results from the pre-training test to the post-training test, but the final test score dropped. Even though the scores dropped they were slightly higher than the pre-training test scores. It could be presumed that the time frame between the post-training test and final test caused the drop in performance, but Group A showed a similar pattern in results which might negate this assumption. Further study needs to be done to see if increased or decreased time intervals between events would make a greater difference or if the information covered in the simulated events needs to be modified to address any discrepancies among the questions. As noted in Chapter 4, the questions that showed the greatest difference between groups were those questions that covered phishing and social engineering.

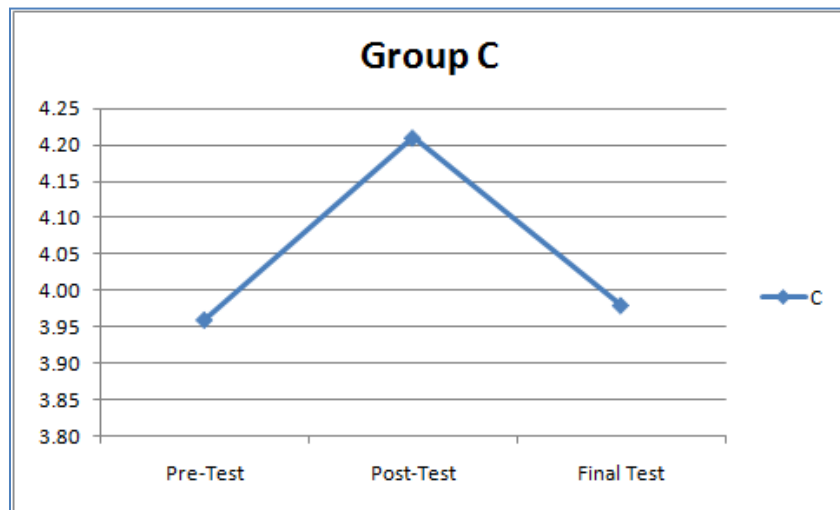


Figure 40 - Line Graph of Group C Data

The patterns for Groups A, B, and C across the tests show that an initial increase in performance was recorded once the groups completed one of the information security awareness training with simulated scenarios events. Once this was achieved, the scores eventually declined to almost the same test scores recorded at the beginning of the research study. It may be posited that the length of the information security awareness training with simulated scenarios that occurred after the pre-training test produced greater results than the shorter periodic training events. There was a minor drop in scores at Week 6 which then returned to higher scores at Week 9. Figure 41 shows the scores for Groups A, B, and C for the initial pre-training test, post-training test, and the final test. Experimental Group A and control Group C showed an initial increase in test scores from the pre-training test and post-training test. Both Groups A and C were given the initial security training. Group B had no change

between the pre-training test and post-training test, but did show an increase at the final test after completing the follow-up training and testing events.

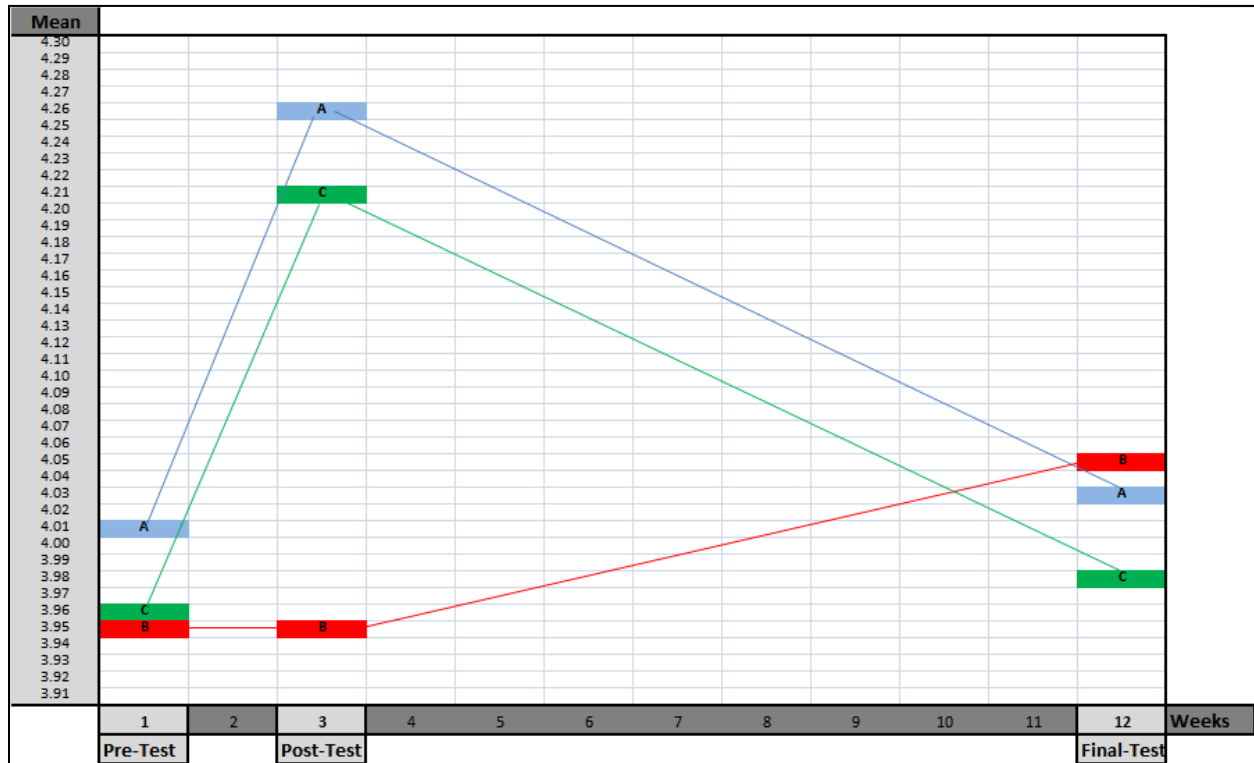


Figure 41 – Groups A, B, and C Test Scores

Conclusions

Ultimately the results are not conclusive, and do not show that the information security awareness training with simulated scenarios and follow-up testing produced lasting significant increases in test score performance. There was a change between the pre- and post-training test for the groups, and Groups A and C did show a difference at the 10% level of significance. This may imply that the groups who received the initial training did show some improvement but, this improvement practically vanished by the end of the research study at the final test. At

the 5% level, the findings throughout showed that the null hypotheses were not rejected and that no significant difference existed between the experimental and control groups. Therefore, all of the research hypotheses cannot be confirmed except at the 10% level for the first research hypothesis that there would be a significant difference between the groups that received the information security awareness training. Even after close examination of the demographic data, there is no substantial difference between the groups and they are comparatively equally represented by their computer experience and background.

A noticeable attribute of the groups is the relatively high scores from the outset of the research study. There was little variance between the groups, with the lowest mean of any group equal to 3.95 out of 5 and the highest mean of any group equal to 4.63 out of 5. Table 27 shows the means of the groups for the tests and the means of all of the groups and all of the tests. From this table we can see that the differences are not significant particularly for the final test. The range of scores on the final test differs by only 0.06 between the lowest and highest values. This was unexpected as the assumption was that the subject who received the simulated information security awareness training and testing would have had higher test scores.

Table 27 - Mean Scores for All Groups and All Tests

Mean Scores for All Groups and All Tests						
Group	Pre-Test	Post-Test	Week 3	Week 6	Week 9	Final
A	4.01	4.26	4.52	4.22	4.63	4.03
B	3.95	3.95	4.32	4.18	4.23	4.04
C	3.96	4.21				3.98
D						3.99
Average:	3.97	4.14	4.42	4.20	4.43	4.01

From the literature review in Chapter 2, the concept of applying deterrence theory, that organizations can reduce computer abuse by implementing standard security policy measures such as anti-virus systems, password protection schemes, rigorous enforcement of computer security policies, and fostering security awareness in employees through special security education (Lee, 2003) was not proven to be necessarily true. Also, Whitman posited that awareness of security risks and the necessary education and training about information security and organizations needs to be increased to avoid accidental and careless mistakes and to increase the effectiveness of their security policies (Whitman, 2004). This statement by Whitman was not proven to be necessarily true from this research study. Even though the research did not prove that simulated security awareness training and testing significantly increased the performance of the subjects from the beginning to the end, the commitment to training end users on information security is still needed. Perhaps if the simulated information security awareness and compliance training had not been performed, then the test results would have decreased over time. Also, according to the 2009 CSI/FBI survey, 53 percent of the respondents say that their organizations allocate 5 percent or less of their overall information

technology budget to information security, and 42 percent spend less than 1 percent of their security dollars on awareness programs which is an alarmingly low expenditure rate when you consider the cost of dealing with security breaches (Richardson, 2008). The fact that approximately \$0.50 for every \$1,000 spent on information technology is spent on information security reveals the need for more focus on awareness education, training, and continuous and random testing. This statement needs further analysis and modification to account for the results of the study, but that does not imply that the training is not needed or could not be effective. To this end, members of a V-CoP must be properly trained and tested to ensure that they not only understand the major security issues of any information system, but that they follow these policies. Von Solms and Von Solms acknowledged that users cannot be held responsible for security problems if they are not told what such security problems are and what they should do to prevent them (Von Solms and Von Solms, 2004). This means that the training is needed, but the form and delivery may need to be modified until the desired results are obtained. This may also have implications for the utilization of simulation. In a simulated environment, users can be exposed to simulated security incidences and threats without compromising their systems or their organizations' systems. Organizations do not want their employees to learn proper information security practices the hard way by opening an infected email that contains a live virus that would infect their system. Lastly, information security will continue to be a major focus that organizations need to address and also that the primary causes of information security breaches are end-user carelessness and mistakes (Baker, 2008), which necessitates computer security awareness training and compliance testing.

Future Research

This dissertation suggests that there are a number of areas for further research that should be done. The following information will address each area of potential future research, why this research is important, and a rationale for each recommendation.

To check for the effect of simulation on the groups another research study could be done with the experimental group receiving the training with the simulated scenarios and the control group receiving the training without the simulated scenarios. This would help to determine if the simulation used in the study would make a positive difference on how the experimental group responded to the follow-up testing. This study would not require making any changes to the system and could be combined with some of the other possible future research areas.

Since this study was done using a highly educated and computer savvy group of subjects, future research should look at a mix of backgrounds. Including less educated subjects with more educated subjects that are involved in a V-CoP may produce different results. This research would be useful to determine what effect education has on information security awareness training retention. Since many organizations are staffed with individuals that at most possess a bachelor's degree, this research would be directly beneficial to employers with V-CoP's staffed with employees with less formal education, since the subjects of this research possessed at least a master's degree. Also, employees with basic computer skills may provide different results, since a majority of the subjects in this research had taken at least one

computer class (29/32), owned two or more computers (26/32), and almost half of the subjects had taken a computer programming course (14/32) which shows a more advanced level of computing knowledge. Almost any piece of information collected from the demographic survey could be further examined by focusing on that particular demographic identifier but for the purpose of future research, suggesting only more or less knowledge of computer systems would be recommended.

The research subjects were faculty from higher education which narrows the findings to this particular group from the science fields making it difficult to extrapolate the results to other groups or groups that are comprised of members from a more varied environment. Even if another study were to be done using college staff rather than college faculty, the results may be different. The research did not take into account diversity of job roles and further study would be useful, even within an educational framework, to determine if members of V-CoPs that included subjects of varying job roles and/or responsibilities might result in different findings. This may be particularly useful in a non-educational setting, such as a corporation that is widely engaged in the use of V-CoPs and needs to ensure that valuable information is kept secure. Simulated information security awareness training and compliance testing would be particularly important in organizations where confidentiality and secrecy are critical and necessary to the operation of the organization (such as the Department of Defense, research and development groups, etc.).

The length of time of the study could be adjusted to be either longer or shorter since the subjects improved from the pre- to post-training test after the lengthy initial simulated

information security awareness training. This could be applied not only to the overall length of the study, but to the length of the training with simulated scenarios events. If the initial simulated information security awareness training was the cause of the improvement in the testing scores between the pre- and post-training tests, then determining the length of each event to maximize effect would be useful. Also, extending the length of the research study to a year or longer, may reveal different results than were obtained by looking at a twelve-week time frame. Pinpointing the optimum time frame may provide significant benefits and keep organizations from wasting time, money, and other valuable scarce resources. Also, in a longer time period, the number and length of events could be adjusted to maximize the effect of the training with simulated scenarios and testing.

Also, increasing the fidelity of the simulations used in the training and testing should be examined to determine if a more advanced and more interactive simulation would change the results of the research. Increased fidelity may assist organizations in determining what level of fidelity is needed to obtain the maximum impact from training with simulated scenarios and testing on V-CoPs or on any user group. The training with simulated scenarios and testing, if successfully adjusted to the maximum fidelity levels, could even be commercialized and used in any organization to train its employees in proper security practices and to reinforce the security policy of the organization.

Lastly, the information security awareness training with simulated scenarios and testing could be modified to be intelligent, adapting to the particular needs of the subject. Adaptive training has been used when a subject is not performing at the desired level in a certain information security subject area.

To improve their score, more training could automatically be provided in the specific problem area. Each test question missed could be used to provide further training until the user scores at the specified level. In one research article, adaptive training was found to produce substantial and sustained gains in students that were engaged in the adaptive training, even six months after the training (Denning, et al., 2009).

APPENDIX A: DEMOGRAPHIC SURVEY

Demographic Survey

Each numbered item records information that will be used in the study. No identifying information will be collected or distributed.

For questions with a dropdown box make sure to click on the down arrow and select the appropriate answer.

When you have completed the survey, click on the Done button at the end and you will be returned to the training web site.

1. Subject ID: (type in the ID you were emailed)
2. Gender (Male or Female)
3. Age (click on the down arrow to select an age range):
4. Current Occupation (click on the down arrow to select an occupation):
5. If faculty, current teaching area:
6. Highest level of education:
7. Number of computer classes taken:
8. Type of computer classes taken:
9. How many computers do you own?
10. How would you rate your experience with computers?
11. How often do you check email?
12. How often do you use instant messaging (IM)?
13. How often do you use Internet research for classes or work?
14. Do you use any social networking sites?
15. If you use social networking sites, which of the following do you use (select all that apply)?
16. Do you upload files on to the web?
17. If you upload files, how often?
18. Do you have anti-virus software installed on your home computer?
19. If you have anti-virus software installed, is it up to date (do you update the software at least monthly)?
20. Do you have a firewall or other device installed to protect your home computer?
21. If you have a firewall or other device, what type is it?
22. Have you ever had your computer infected by a computer virus, or had someone
23. hack your computer?
24. If your computer was infected, what type of infection was it?
25. Do you have your own web site that you manage?
26. How often do you change your password for accessing password protected sites?

APPENDIX B: TESTS TAKEN BY RESEARCH SUBJECTS

Pre-Training Test and Final Test

Answer each of the following questions by selecting the letter of the answer that you think is correct. Select only one answer for each question. Use the drop down box to the right of each question to select your answer (a, b, c, d, or e)

There are 20 questions after you enter your ID. All of the questions are required. When you are finished, you will automatically be sent back to the main study web site.

Thank you for participating in this research study.

(1 = Least secure or worst answer, 5 = Most secure or best answer)

1. Anti-virus software should be installed on all computers.
 - a) True (5)
 - b) False (1)
 - c) Depends if the computer is connected to the Internet (4)
 - d) Depends on who uses the computer (2)
 - e) Anti-virus software is not necessary if the computer has a firewall (3)

2. Users should change their password to a password protected site every ____?
 - a) day (2)
 - b) week (4)
 - c) month (5)
 - d) 6 months (3)
 - e) year (1)

3. A strong password is a password that contains which of the following?
 - a) letters (1)
 - b) letters and numbers (3)
 - c) letters and non-numeric characters (4)
 - d) letters, numbers, and non-numeric characters (5)
 - e) upper case and lower case letters (2)

4. When sharing a file with someone else over the Internet, which one of the following procedures should you follow?
 - a) Make sure that you know the person on the receiving end. (5)
 - b) Make sure that you encrypt the information before sharing. (4)
 - c) Never send confidential information over the Internet. (2)
 - d) Don't upload the information to a shared site. (1)
 - e) Make sure that you review the data before sharing. (3)

5. When opening an email message attachment, you should always do this before opening the attachment?

- a) Make sure that you know the person that sent the email (4)
- b) Make sure that the attachment is not an executable file (3)
- c) Open the attachment if it is from an email address within your organization (2)
- d) Only open if you have scanned it for viruses (5)
- e) Never open email attachments (1)

6. If you upload a file to a shared but secured site, it is acceptable to share confidential data as long as what is true?

- a) The file does not contain social security numbers. (3)
- b) The file contains older data that is not current. (2)
- c) The file has been approved for viewing by the members of the secured site. (5)
- d) The file has been properly checked for errors and inconsistencies. (4)
- e) Never upload confidential data to a shared site, even if it is secure. (1)

7. Email is confidential, and cannot be used against an employee, student, etc.

- a) True (1)
- b) False (5)
- c) True, as long as the email is sent using a personal email account. (3)
- d) False, if the user sends the email from work. (4)
- e) False, if the user sends the email from a public computer system. (2)

8. What is the best way to protect your computer, files and data from being infected by a computer virus?

- a) Keep anti-virus software up to date. (5)
- b) Don't have a connection to the Internet. (1)
- c) Don't download files or open files from any web site. (3)
- d) Have a firewall installed between your computer and the Internet. (4)
- e) Keep a backup of all critical software programs. (2)

9. What is computer phishing?

- a) The process of looking for confidential data on a remote computer system. (3)
- b) The process of seeking to gain access to another computer system. (4)
- c) The fraudulent process of attempting to acquire sensitive information. (5)
- d) The process of passing along a computer virus from one web site to another web site. (2)
- e) The fraudulent process of trying to steal computer configuration codes. (1)

10. Confidential data that is no longer needed or used should be?
- a) Destroyed when no longer needed or out of date. (4)
 - b) Backed up and stored for later use. (2)
 - c) Stored on a system that is used for archiving purposes. (3)
 - d) Printed out and then destroyed on the computer system. (1)
 - e) Deleted and permanently erased from all computer systems (5)
11. Which one of the following, in your opinion, is the biggest risk of data sharing on the Internet?
- a) Sharing confidential data on a secure site. (3)
 - b) Sharing non-confidential data on a community site. (1)
 - c) Hackers knowledge of the existence of the community site. (4)
 - d) Sharing confidential data on a community site. (5)
 - e) Sharing executable files on a secure site. (2)
12. If a member of the information technology group at your organization calls and asks for confidential data you should do which one of the following?
- a) Ask them to provide proof of their identity. (4)
 - b) Provide them with the information they requested in writing. (2)
 - c) Provide them with the information they requested verbally. (1)
 - d) Don't give them the confidential data, they shouldn't be asking. (5)
 - e) Ask to speak to their supervisor to verify the necessity of this information. (3)
13. It is not necessary to have a password on your mobile devices like a PDA (e.g. Palm Pilot), cell phone, laptop, etc. since you should always keep these devices in your position or locked away?
- a) True. (1)
 - b) False. (5)
 - c) True, as long as they are kept secure. (3)
 - d) False, since it is impossible to always keep these devices in your position or locked up.(4)
 - e) False, because passwords just make it more difficult to use the devices. (2)
14. What should you do if you notice someone that you don't know using a co-workers computer?
- a) It is probably just a new person from the IT department, just ignore them. (1)
 - b) Question them and ask why they are there. (5)
 - c) Call the police. (3)
 - d) Get another employee and then approach this person. (4)
 - e) Send an email to the IT department to see if they have an employee working on your co-workers computer. (2)

15. When backing up or making copies of your data which strategy should you follow?
- a) Back up everything, data and programs. (3)
 - b) Back up only the data that you use on a regular basis. (4)
 - c) Back up data from the My Documents folder only. (1)
 - d) Back up all data at least once, and then changed data as needed. (5)
 - e) Back up all data once per year. (2)
16. If you discover that a computer security breach has occurred you should?
- a) Immediately notify your information technology department. (5)
 - b) Shut down your computer so that it is not vulnerable to the breach. (4)
 - c) Call the FBI or other law enforcement agency to report the breach. (1)
 - d) Notify the president of your organization so that they can take appropriate action. (2)
 - e) Run a virus scan on your computer to see if you have been infected with a virus. (3)
17. How often should data be deleted from a shared web site?
- a) On a monthly basis. (2)
 - b) When it is no longer regularly used by members of the site. (4)
 - c) It depends on the confidential nature of the data. (3)
 - d) Never, it should be archived and made available. (1)
 - e) When it is no longer relevant to the core mission of the shared web site. (5)
18. A "strong" password to a shared site should be ___ characters in length.
- a) 6 (1)
 - b) 8 (2)
 - c) 10 (3)
 - d) 12 (4)
 - e) 14 (5)
19. To prevent unauthorized access to data on your computer or portable device, you should utilize a password and what other computer security practice?
- a) Set up a VPN connection on your device. (2)
 - b) Make sure that you have a spam filter on the device. (1)
 - c) Utilize the firewall features of the device. (3)
 - d) Encrypt the data on the device. (5)
 - e) Make sure that antivirus software is installed on the device. (4)
20. What is the average cost of a security breach that involved financial fraud?
- a) \$10,000 per incident. (1)
 - b) \$50,000 per incident. (2)
 - c) \$100,000 per incident. (3)
 - d) \$250,000 per incident. (4)
 - e) \$500,000 per incident. (5)

Post-Training Test

Answer each of the following questions by selecting the best answer.

Answer each of the following questions by selecting the letter of the answer that you think is correct. Select only one answer for each question (a, b, c, d, or e).

(1 = Least secure or worst answer, 5 = Most secure or best answer)

1. What should be installed on all computers to help protect the computers from worms and Trojans?
 - a) Anti-Virus software (5)
 - b) Office software (1)
 - c) Malware software (3)
 - d) Spam filtering software (2)
 - e) Firewall software (4)

2. How often should you change your password?
 - a) Every 15 days (5)
 - b) Every 6 weeks (4)
 - c) Every 3 months (3)
 - d) Every 6 months (2)
 - e) Once a year (1)

3. What makes a “strong” password?
 - a) Passwords that are dictionary words (1)
 - b) Passwords that use letters and numbers (3)
 - c) Passwords that use letters and non-numeric characters (4)
 - d) Passwords that use letters, numbers, and non-numeric characters (5)
 - e) Passwords that use upper case and lower case letters (2)

4. What should you do when you share a file on the Internet?
 - a) Make sure that the person on the receiving end is known to you. (5)
 - b) Encrypt the information before sharing it on the Internet. (4)
 - c) Be careful to never send confidential information over the Internet. (2)
 - d) It is better not to upload information to a shared site. (1)
 - e) Carefully review the data before sharing. (3)

5. If you receive an email with an attached file, what should you do?
 - a) Identify the person that sent the email (4)
 - b) Make sure that you know the type of file that is attached (3)
 - c) Open the attachment if it is from someone within your organization (2)
 - d) Open the file if you have properly scanned it for viruses (5)
 - e) It is safe to open email attachments (1)

6. Sharing confidential data to a shared Internet site is acceptable if which one of the following is true?
- a) The file does not contain social security numbers. (3)
 - b) The file contains older data that is not current. (2)
 - c) The file has been approved for viewing by the members of the secured site. (5)
 - d) The file has been properly checked for errors and inconsistencies. (4)
 - e) Never upload confidential data to a shared site, even if it is secure. (1)
7. Email is the property of the sender, even at work.
- a) True (1)
 - b) False (5)
 - c) True, as long as the email is sent using a personal email account. (3)
 - d) False, if the user sends the email from work. (4)
 - e) False, if the user sends the email from a public computer system. (2)
8. How should you protect your computer, files and data from being infected by a computer virus?
- a) Keep anti-virus software up to date. (5)
 - b) Don't have a connection to the Internet. (1)
 - c) Don't download files or open files from any web site. (3)
 - d) Have a firewall installed between your computer and the Internet. (4)
 - e) Keep a backup of all critical software programs. (2)
9. Computer phishing is the process of doing what?
- a) The process of looking for confidential data on a remote computer system. (3)
 - b) The process of seeking to gain access to another computer system. (4)
 - c) The fraudulent process of attempting to acquire sensitive information. (5)
 - d) The process of passing along a computer virus from one web site to another web site. (2)
 - e) The fraudulent process of trying to steal computer configuration codes. (1)
10. Data of a confidential nature that is no longer needed or used should be?
- a) Destroyed when no longer needed or out of date. (4)
 - b) Backed up and stored for later use. (2)
 - c) Stored on a system that is used for archiving purposes. (3)
 - d) Printed out and then destroyed on the computer system. (1)
 - e) Deleted and permanently erased from all computer systems (5)
11. Which of the following would you say is the biggest risk of data sharing on the Internet?
- a) Sharing confidential data on a secure site. (3)
 - b) Sharing non-confidential data on a community site. (1)
 - c) Hackers knowledge of the existence of the community site. (4)
 - d) Sharing confidential data on a community site. (5)
 - e) Sharing executable files on a secure site. (2)

12. Mary from the information technology calls and asks for confidential data. What should you tell Mary?

- a) Ask them to provide proof of their identity. (4)
- b) Provide them with the information they requested in writing. (2)
- c) Provide them with the information they requested verbally. (1)
- d) Don't give them the confidential data, they shouldn't be asking. (5)
- e) Ask to speak to their supervisor to verify the necessity of this information. (3)

13. Passwords are not necessary on mobile devices like a PDA (e.g. Palm Pilot), cell phone, laptop, etc. Is this statement true or false?

- a) True. (1)
- b) False. (5)
- c) True, as long as they are kept secure. (3)
- d) False, since it is impossible to always keep these devices in your position or locked up. (4)
- e) False, because passwords just make it more difficult to use the devices. (2)

14. A person you are not familiar is using one of your co-workers computers that is out sick. What would be the most appropriate course of action for you to take?

- a) It is probably just a new person from the IT department, just ignore them. (1)
- b) Question them and ask why they are there. (5)
- c) Call the police. (3)
- d) Get another employee and then approach this person. (4)
- e) Send an email to the IT department to see if they have an employee working on your co-workers computer. (2)

15. What is the most appropriate strategy for backing up your computer data?

- a) Back up everything, data and programs. (3)
- b) Back up only the data that you use on a regular basis. (4)
- c) Back up data from the My Documents folder only. (1)
- d) Back up all data at least once, and then changed data as needed. (5)
- e) Back up all data once per year. (2)

16. What should you do if you discover a computer security breach at your place of work?

- a) Immediately notify your information technology department. (5)
- b) Shut down your computer so that it is not vulnerable to the breach. (4)
- c) Call the FBI or other law enforcement agency to report the breach. (1)
- d) Notify the president of your organization so that they can take appropriate action. (2)
- e) Run a virus scan on your computer to see if you have been infected with a virus. (3)

17. How frequently should data be removed from a shared web site?

- a) On a monthly basis. (2)
- b) When it is no longer regularly used by members of the site. (4)
- c) It depends on the confidential nature of the data. (3)
- d) Never, it should be archived and made available. (1)
- e) When it is no longer relevant to the core mission of the shared web site. (5)

18. A “strong” password to a shared site should be how many characters in length?

- a) 6 (1)
- b) 8 (2)
- c) 10 (3)
- d) 12 (4)
- e) 14 (5)

19. To help to prevent unauthorized access to data on your computer or portable device, you should use a password and?

- a) Set up a VPN connection on your device. (2)
- b) Make sure that you have a spam filter on the device. (1)
- c) Utilize the firewall features of the device. (3)
- d) Encrypt the data on the device. (5)
- e) Make sure that antivirus software is installed on the device. (4)

20. Computer security breaches that involved financial fraud cost on average _____ per incident.

- a) \$100,000 per incident. (4)
- b) \$500,000 per incident. (5)
- c) \$1,000,000 per incident. (3)
- d) \$2,500,000 per incident. (2)
- e) \$5,000,000 per incident. (1)

Week 3 Follow-Up Test

Answer each of the following questions by selecting the letter of the answer that you think is correct. Select only one answer for each question. Use the drop down box to the right of each question to select your answer (a, b, c, d, or e)

There are 7 questions after you enter your ID. All of the questions are required. When you are finished, you will automatically be sent back to the main study web site.

Thank you for participating in this research study.

1. Joe has been using the same password for that last 6 months. His password is the word scubadiver because he is really into scuba diving and his password is easy to remember. What type of password is Joe using?

- a) A weak password (5)
- b) A medium password (4)
- c) A strong password (2)
- d) A difficult password (3)
- e) A hack proof password (1)

2. Julie has recently joined a Virtual Community of Practice for a project she is working on at her company. The company has sites located throughout the US, Canada and England. Recently, a new member of the community located in England, Mark, has been requesting documents that are increasingly confidential in nature. Julie is not comfortable with Mark's latest requests for information. What should she do?

- a) Double check the identity of the person making the requests. (4)
- b) Encrypt the information before sharing with Mark using the companies encryption tool (3)
- c) Don't provide the requested information to Mark. (5)
- d) Check with the administrator of the virtual community to make sure that the site is secure. (2)
- e) Ask Mark for more information on why he needs this data. (1)

3. You receive an email from the systems administrator of the V-CoP asking for your Employee ID and your drivers' license number for verification purposes. You notice the return address seems to be from your company. What should you do?

- a) Do not respond to the email – this is probably a phishing attempt. (5)
- b) Call the system administrator and see if he/she needs that information. (4)
- c) Send them your employee ID but not your drivers' license number. (1)
- d) Ask the systems administrator for more information by responding to the email (2)
- e) Respond to the email stating that you will not provide the information. (3)

4. Dr. Smith has a desktop computer and a laptop that he uses at work. The laptop he takes home and uses on his home network, and he also uses it at conferences and when he is at public sites where he can get wireless access. Recently, a local coffee shop has told customers to be wary of using their wireless network since some customers have complained about having their computers infected with viruses and/or hacked by computer hackers. What should Dr. Smith do to protect his laptop?

- a) Make sure his anti-virus software is always up to date. (3)
- b) He shouldn't connect to the Internet from the coffee shop. (5)
- c) He shouldn't download files or open files from the web. (2)
- d) Make sure that he has a firewall installed on his laptop. (4)
- e) Make sure that he has a backup of all critical software programs. (1)

5. Dr. Jones, the head of the Biology Department at Central University, received an email from the information technology department. The email stated that all employees of Central University needed to provide their user account information (login and password) along with other information such as email address, home address information, etc. They claim this is part of the project to make sure that data is kept secure. How should Dr. Jones respond to this request? The email seems to be from an address within the organization.

- a) Respond to the request since it is from an email address from within the University. (1)
- b) Respond to the request, but don't provide his password. (2)
- c) Just ignore the email. (4)
- d) Contact the information services department to see if they sent the email. (5)
- e) Reply to the email and ask the person to provide proof of their identity. (3)

6. Henry has been sending a lot of personal email from work. He is not using his work email system, but logs on to Yahoo.com and uses his Yahoo email account. Henry is not happy at his job and has been sending negative emails about his boss and the management of the company. Henry doesn't think he has anything to worry about since he is not using his work email so it is his property. Is Henry correct?

- a) Yes, it is his account so there is no problem (3)
- b) Yes, because his employer does not have a legal right to look at messages coming to and from his Yahoo account. (2)
- c) No. Even though Henry is using his private email account, the messages are being sent on the company's network. (5)
- d) No, email is never private anywhere. (4)
- e) Yes, email is always private. (1)

7. Employees of Sure-Tight Systems do contract work for the Department of Defense, and a few other government agencies. Dr. Tompkins, head of research, maintains copies of all data he is collecting for one of the projects on human performance. What method of backup should he follow so that his data is not at risk of being lost?

- a) Back up everything on his computer, data and programs. (2)
- b) Back up only the data that he uses on a regular basis. (4)
- c) Back up data from his My Documents folder only. (1)
- d) Back up all data on his computer at least once, and then changed data as needed. (5)
- e) Back up all of his data once per quarter (every 3 months). (3)

Week 6 Follow-Up Test

Answer each of the following questions by selecting the letter of the answer that you think is correct. Select only one answer for each question. Use the drop down box to the right of each question to select your answer (a, b, c, d, or e)

There are 7 questions after you enter your ID. All of the questions are required. When you are finished, you will automatically be sent back to the main study web site.

Thank you for participating in this research study.

1. The IT help desk has called you because they are performing a trace of all data packets that come in and out of the corporate network. The employee, Joanne, has asked for your user account name and password that you are currently using so that she can map the packets that are coming from and going to your computer system. What should you tell Joanne?"

- a) Give her the information since she states she is from the IT department. (1)
- b) Verify that there really is a Joanne that works for the IT department first. (3)
- c) Ask Joanne a couple of questions that only an employee of the company should know. (2)
- d) Don't give Joanne the information since she should already have that information. (5)
- e) Tell her that you will call her back after you clear this with your supervisor. (4)

2. U State has recently started a virtual community of practice web site for its incoming assistant professors. Jean, a recent hire in the fine arts department, has been using the site to see how other faculty are handling teaching and research, and related issues. Another faculty on the site, Jeremy, has been asking for examples of exams so that he can get ideas for his tests. Jean doesn't know Jeremy since he is on another campus and in another department. What should she do if she decides to share an exam with Jeremy?

- a) She should make sure that she verifies Jeremy's identity before sharing. (5)
- b) She should encrypt the information before sharing. (3)
- c) She should not send confidential information over the Internet, even to this site. (4)
- d) She shouldn't upload the information to a shared site. (2)
- e) She should review the data before sharing it with Jeremy. (1)

3. Phyllis has been emailing information to colleagues at the Burun Research Facility in Seattle, WA for the past 2 years. She is a research chemist at M State, and has been collecting data on experiments she is running in collaboration with Burun. Yesterday, she received an email from a new employee she doesn't know at Burun who attached a file that has a new protocol that she is supposed to follow. How should she handle this email?

- a) Make sure that she knows the person that sent the email (5)
- b) Make sure that the attachment is not an executable file (4)
- c) Open the attachment if it is from an email address within the organization (1)
- d) Only open the file if she has scanned it for viruses (3)
- e) Never open email attachments (2)

4. Georgia State College loans laptop computers to faculty and staff who are on sabbatical, or who need to work away from campus or at home. Dr. Wilmer is doing some work for the Department of Defense and needs a laptop while he is visiting the Pentagon in Washington, DC. He is a bit concerned about using the laptops from the college as they are shared by many different college employees. He has heard of some faculty picking up viruses from these shared computers. What would be the most effective way to protect his data while using the laptop?

- a) Make sure the anti-virus software is up to date. (5)
- b) He shouldn't connect to the Internet while using the laptop. (2)
- c) He shouldn't download files or open files from any web site. (3)
- d) He should make sure that the laptop has a firewall installed on the computer. (4)
- e) He should make a backup of all critical software programs on the laptop.(1)

5. Y State created a web portal community for faculty to share best practices for teaching and student learning strategies. Allen, an active participant of the community, has used the site to get lots of good instructional ideas for his classes. Yesterday, he received a phone call from an IT support staff asking for his username and password to the site because they need to do maintenance on the site. How should Allen respond to this request?

- a) Do not respond to the call – this is probably a phishing attempt. (5)
- b) Call the system administrator and see if he/she really needs that information. (4)
- c) Send his user name, but not his password. (1)
- d) He should ask for more information before responding. (2)
- e) He should respond to the call by stating that he will not provide the information. (3)

6. Eloise is a member of the English Community of Practice shared online site at her college. Part of the site requires a username and password to gain access. Eloise has only changed her password once since joining 2 years ago. Her current password is 3@CHauCeR3. What type of password is she using?

- a) A weak password (2)
- b) A medium password (4)
- c) An easy password (3)
- d) A strong password (5)
- e) A hack proof password (1)

7. You have been working on some important research for your next major conference in biotechnology. You have been saving some of the data to a USB drive, and some to your hard drive. What would be the most effective method to follow so that your data is backed up properly?

- a) Back up everything, data and programs (4).
- b) Back up only the data that you use on a regular basis (3).
- c) Back up data from the My Documents folder only. (2)
- d) Back up all data at least once, and then changed data regularly. (5)
- e) Back up all data once per year. (1)

Week 9 Follow-Up Test

Answer each of the following questions by selecting the letter of the answer that you think is correct. Select only one answer for each question. Use the drop down box to the right of each question to select your answer (a, b, c, d, or e)

There are 7 questions after you enter your ID. All of the questions are required. When you are finished, you will automatically be sent back to the main study web site.

Thank you for participating in this research study.

1. Which ONE of the following passwords would you consider to be the strongest?

- a) 1New@PassworD (5)
- b) 23Smith45 (2)
- c) 9@fghl7 (4)
- d) 1newpassword23 (1)
- e) PassWorD23 (3)

2. Your school wants you to participate in a new community of practice that connects teachers with interested students to help "mentor" them through their college experience. A new student named Gloria has been assigned to you. You have never met Gloria, but she seems very excited about college and learning as much as she possibly can. Recently, Gloria has asked you for personal information - where you live, names of your kids, type of car you drive, etc. You don't feel comfortable sharing this information, even though you believe Gloria is harmless. How should you handle Gloria's requests?

- a) Make sure that you really know the person on the receiving end. (3)
- b) First ask Gloria to provide personal information to you. (1)
- c) Don't provide Gloria with this information. (5)
- d) Ask Gloria why she wants this information? (4)
- e) As long as the information is not too personal feel free to share. (2)

3. Dr. Fleming has been working remotely over the past 3 months as part of her field work in marine biology. She regularly goes to the local library to use their wireless access. However, she is concerned that she might pick up a virus since the library does not require secured access to their wireless network (anyone can use it). What would be her best method of protecting her computer from getting a virus?

- a) Keep her anti-virus software up to date. (5)
- b) Don't use the connection to the Internet. (2)
- c) Don't download files or open files from any web site. (3)
- d) Have a firewall installed on her computer. (4)
- e) Keep a backup of all critical software programs. (1)

4. Dr. Holmes is looking for information on biochemical reactions in insects. He has found a number of sites that have appropriate information but one in particular seems to have exactly what he wants. However, to access the site he is required to provide personal information that doesn't seem to be warranted for what he needs. He thinks this may be a phishing site. What would make him think the site is a phishing site?

- a) The site is looking for confidential data on a remote computer system. (4)
- b) The site is seeking to gain access to another computer system. (3)
- c) The site is trying, fraudulently, to attempt to acquire sensitive information. (5)
- d) The site is trying to pass along a computer virus from one web site to another web site. (2)
- e) The site is fraudulently trying to steal computer configuration codes. (1)

5. Jerry is a new employee at your school and is concerned about privacy issues regarding his students and their records. He has asked you to respond to concerns about information compromises that have occurred at other colleges and universities. He wants to share information with his colleagues but is concerned about the safety of this "shared" information. What would you tell him, in your opinion, is the biggest risk of data sharing on the Internet?

- a) Sharing confidential data on a secure site. (4)
- b) Sharing non-confidential data on a community site. (1)
- c) Hackers knowledge of the existence of the community site. (3)
- d) Sharing confidential data on a community site. (5)
- e) Sharing executable files on a secure site. (2)

6. You have been put in charge of making sure that proper backups of data from the virtual community of practice in anthropology are being made. Which one of the following strategies would you recommend following?

- a) Back up everything, data and programs. (3)
- b) Back up only the data that you use on a regular basis. (4)
- c) Back up data from the My Documents folder only. (1)
- d) Back up all data at least once, and then changed data as needed. (5)
- e) Back up all data once per year. (2)

7. Dr. Thomas from the chemistry department has received an email from someone in the college. He doesn't know this person, but the email states that the attachment is important information regarding the schools retirement plan. The email also states that there is time sensitive information in the attachment that must be replied to by 5pm today. How should Dr. Thomas respond to this email, or what should he do before he opens the attachment?

- a) Make sure that you know the person that sent the email (4)
- b) Make sure that the attachment is not an executable file (3)
- c) Open the attachment if it is from an email address within your organization (2)
- d) Only open if you have scanned it for viruses (5)
- e) Never open email attachments (1)

APPENDIX C: DATA COLLECTED DURING RESEARCH STUDY

Table 28 – Pre-Training Test Data

PRE-TEST RESULTS																						
ID	Subject Questions	(Number and rank order)																		Mean	Median	Std Dev
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18			
A1	a 5 d 3 d 5 b 4 d 5 e 1 b 5 d 4 c 5 a 4 b 1 d 5 b 5 e 2 d 5 a 5 c 3 b 2 e 4 a 1	3.7	4.0	1.5																		
A2	a 5 b 4 d 5 e 3 d 5 e 1 d 4 a 5 c 5 a 4 d 5 e 3 d 4 b 5 d 5 a 5 e 5 e 5 d 5 d 4	4.4	5.0	1.0																		
A3	a 5 c 5 d 5 b 4 d 5 e 1 b 5 a 5 c 5 e 5 d 5 d 5 d 4 b 5 d 5 a 5 c 3 b 2 c 3 c 3	4.3	5.0	1.2																		
A4	a 5 d 3 d 5 c 2 d 5 c 5 b 5 a 5 c 5 e 5 d 5 b 2 b 5 b 5 d 5 a 5 e 5 c 3 c 3 c 3	4.3	5.0	1.1																		
A5	a 5 d 3 d 5 a 5 d 5 e 1 b 5 a 5 a 3 e 5 d 5 d 5 d 4 e 2 a 3 a 5 e 5 b 2 a 1	3.8	5.0	1.5																		
A6	a 5 c 5 b 3 d 1 d 5 e 1 d 4 a 5 c 5 b 2 d 5 d 5 d 4 e 2 d 5 a 5 e 5 d 4 c 3	3.8	4.5	1.5																		
A7	a 5 d 3 d 5 a 5 b 3 e 1 b 5 e 2 c 5 e 5 c 4 d 5 b 5 e 2 d 5 b 4 e 5 d 4 c 3 d 4	4.0	4.5	1.3																		
A8	c 4 e 1 d 5 b 4 b 3 c 5 b 5 b 1 c 5 e 5 a 3 d 5 c 3 c 3 d 5 a 5 a 2 e 5 d 5 c 3	3.9	4.5	1.4																		
Mean	4.9	3.4	4.8	3.5	4.5	2.0	4.8	4.0	4.8	4.4	4.1	4.4	4.3	3.3	4.8	4.9	4.1	3.4	3.4	2.8		
Median	5.0	3.0	5.0	4.0	5.0	1.0	5.0	5.0	5.0	5.0	5.0	5.0	4.0	2.5	5.0	5.0	5.0	3.0	3.0	3.0		
SD	0.4	1.3	0.7	1.4	0.9	1.9	0.5	1.6	0.7	1.1	1.5	1.2	0.7	1.5	0.7	0.4	1.2	1.3	1.2	1.2		
B1	a 5 d 3 b 3 c 2 d 5 e 1 b 5 d 4 c 5 a 4 d 5 e 3 d 4 e 2 d 5 a 5 b 4 b 2 a 2 b 2	3.6	4.0	1.4																		
B2	a 5 d 3 d 5 d 1 a 4 e 1 b 5 a 5 c 5 e 5 d 5 d 5 c 3 b 5 d 5 a 5 e 5 b 2 e 4 b 2	4.0	5.0	1.5																		
B3	a 5 d 3 e 2 e 3 d 5 e 1 b 5 a 5 c 5 c 3 d 5 e 3 a 1 b 5 d 5 a 5 c 3 a 1 c 3 a 1	3.5	3.0	1.6																		
B4	a 5 d 3 d 5 c 2 b 3 e 1 b 5 a 5 c 5 e 5 d 5 d 5 b 5 e 2 d 5 a 5 e 5 d 4 d 5 e 5	4.3	5.0	1.3																		
B5	a 5 c 5 b 3 c 2 a 4 c 5 b 5 a 5 c 5 a 4 d 5 e 3 b 5 b 5 a 3 a 5 e 5 c 3 d 5 c 3	4.3	5.0	1.0																		
B6	c 4 c 5 d 5 a 5 b 3 e 1 b 5 c 3 b 4 a 4 d 5 a 4 d 4 d 5 a 5 c 3 b 2 e 4 c 3	3.9	4.0	1.1																		
B7	a 5 c 5 d 5 e 3 d 5 e 1 b 5 a 5 c 5 e 5 d 5 d 5 b 5 d 4 a 3 a 5 e 5 d 4 d 5 b 2	4.4	5.0	1.2																		
B8	a 5 d 3 d 5 e 3 d 5 c 5 d 4 a 5 c 5 c 3 d 5 e 3 b 5 b 5 a 3 b 4 b 4 d 4 d 5 e 5	4.3	5.0	0.9																		
Mean	4.9	3.8	4.1	2.6	4.3	2.0	4.9	4.6	4.9	4.1	5.0	3.9	4.0	4.0	4.3	4.9	4.3	2.8	4.1	2.9		
Median	5.0	3.0	5.0	2.5	4.5	1.0	5.0	5.0	5.0	4.0	5.0	3.5	4.5	4.5	5.0	5.0	4.5	2.5	4.5	2.5		
SD	0.4	1.0	1.2	1.2	0.9	1.9	0.4	0.7	0.4	0.8	0.0	1.0	1.4	1.3	1.0	0.4	0.9	1.2	1.1	1.5		
C1	a 5 d 3 b 3 a 5 a 4 c 5 b 5 a 5 c 5 c 3 d 5 e 3 c 3 b 5 c 1 e 3 b 4 b 2 d 5 a 1	3.8	4.0	1.4																		
C2	c 4 d 3 b 3 a 5 c 2 c 5 c 3 a 5 b 4 a 4 d 5 a 4 b 5 b 5 a 3 e 3 c 3 b 2 e 4 a 1	3.7	4.0	1.2																		
C3	a 5 c 5 d 5 a 5 d 5 c 5 b 5 a 5 b 4 e 5 d 5 d 5 e 2 b 5 a 3 a 5 e 5 b 2 e 4 a 1	4.3	5.0	1.3																		
C4	a 5 d 3 d 5 a 5 d 5 e 1 b 5 a 5 a 3 c 3 d 5 d 5 e 2 b 5 d 5 a 5 c 3 b 2 d 5 d 1	3.9	5.0	1.5																		
C5	a 5 c 5 d 5 a 5 d 5 a 3 b 5 a 5 c 5 e 5 d 5 d 5 b 5 d 4 d 5 a 5 e 5 b 2 d 4	4.5	5.0	1.0																		
C6	a 5 c 5 b 3 a 5 a 4 e 1 d 4 a 5 c 5 a 4 d 5 a 4 b 5 e 2 d 5 a 5 e 5 c 3 d 5 c 3	4.2	5.0	1.2																		
C7	a 5 c 5 d 5 a 5 d 5 c 5 e 2 a 5 a 3 e 5 d 5 e 3 c 3 e 2 d 5 a 5 e 5 c 3 e 4 a 1	4.1	5.0	1.3																		
C8	a 5 d 3 d 5 c 2 b 3 e 1 b 5 a 5 a 3 a 4 d 5 d 5 d 4 e 2 c 1 a 5 b 4 b 2 b 2	3.4	3.5	1.5																		
Mean	4.9	4.0	4.3	4.6	4.1	3.3	4.3	5.0	4.0	4.1	5.0	4.3	3.6	3.8	3.5	4.5	4.3	2.3	3.9	1.8		
Median	5.0	4.0	5.0	5.0	4.5	4.0	5.0	5.0	4.0	4.0	5.0	4.5	3.5	4.5	4.0	5.0	4.5	2.0	4.0	1.0		
SD	0.4	1.1	1.0	1.1	1.1	2.0	1.2	0.0	0.9	0.8	0.0	0.9	1.3	1.5	1.8	0.9	0.9	0.5	1.2	1.2		

Table 29 – Post-Training Test Data

POST-TEST RESULTS																							
Subject Questions																							
ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Mean	Median	Std Dev
A1	c	b	d	b	b	e	d	d	c	a	e	d	b	d	d	a	b	e	e	a	4.0	4.0	1.2
A2	a	c	d	c	d	d	d	a	c	d	d	e	d	b	d	a	e	e	e	d	4.3	5.0	1.2
A3	a	a	d	c	a	e	b	a	c	e	d	d	d	b	d	a	e	e	e	d	4.4	5.0	1.3
A4	a	c	d	c	d	c	b	a	a	e	d	b	b	b	d	a	b	e	e	d	4.5	5.0	1.1
a5	a	b	d	d	a	e	d	a	c	e	d	b	b	e	d	a	e	e	e	d	4.4	5.0	1.1
A6	a	c	d	d	d	e	d	a	c	e	d	d	d	d	d	a	e	e	e	d	4.2	5.0	1.4
A7	a	c	d	a	b	e	b	a	c	e	d	b	b	d	d	a	e	d	d	c	4.3	5.0	1.2
A8	a	e	d	c	d	e	d	b	c	e	e	d	b	b	d	b	e	e	e	d	4.1	5.0	1.4
Mean	4.8	3.3	5.0	2.9	4.3	2.1	4.5	4.4	4.8	4.3	4.3	4.4	4.6	3.5	4.8	4.9	4.8	4.9	4.6	4.4			
Median	5.0	3.0	5.0	2.0	4.5	1.0	4.5	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0		
SD	0.7	1.2	0.0	1.6	0.9	1.6	0.5	1.4	0.7	1.4	1.4	1.2	0.5	1.6	0.7	0.4	0.5	0.4	0.7	1.4			
B1	e	c	b	c	d	c	b	a	c	a	d	e	d	d	b	a	b	e	b	c	3.7	4.0	1.3
B2	a	b	d	c	a	e	d	a	c	e	d	d	d	b	d	a	b	e	b	e	4.2	5.0	1.2
B3	a	c	b	c	d	e	b	a	c	e	c	a	b	b	a	a	d	a	c	a	3.6	4.0	1.5
B4	a	c	d	a	d	e	d	a	c	e	d	d	d	b	d	a	b	d	d	e	4.3	5.0	1.3
B5	a	a	d	b	a	c	b	a	a	a	d	d	b	c	a	a	e	c	c	a	4.2	4.5	1.0
B6	b	1	b	d	d	e	b	e	b	a	e	a	b	d	d	a	c	b	c	b	3.4	4.0	1.5
B7	a	c	d	c	d	e	b	a	c	e	d	d	d	d	a	a	b	d	d	d	4.3	5.0	1.2
B8	a	c	d	e	d	b	b	a	c	e	d	d	d	d	b	b	d	d	d	d	4.0	5.0	1.4
Mean	4.4	3.5	4.3	2.6	4.8	2.1	4.8	4.6	4.6	4.4	4.5	4.3	4.4	4.1	4.1	4.9	4.9	2.8	3.9	3.3			
Median	5.0	3.0	5.0	2.0	5.0	1.0	5.0	5.0	5.0	4.5	5.0	4.5	4.0	4.5	4.5	5.0	3.5	2.5	3.5	4.0			
SD	1.4	0.8	1.0	1.3	0.5	1.8	0.5	1.1	0.7	0.7	1.1	0.9	0.5	1.1	1.0	0.4	1.4	1.2	1.0	1.9			
C1	a	d	d	a	a	e	b	a	a	e	a	e	b	d	a	a	e	e	e	a	4.1	4.5	1.2
C2	e	b	d	b	a	a	b	a	c	b	d	d	b	d	b	a	a	d	e	d	4.1	4.5	1.3
C3	a	c	d	c	d	e	b	a	b	a	d	d	b	b	a	a	e	e	e	e	4.3	5.0	1.2
C4	a	b	d	c	a	e	b	e	a	e	d	d	b	b	a	a	c	e	d	e	4.0	5.0	1.3
C5	c	c	d	a	d	a	b	a	a	b	d	d	b	b	a	a	e	e	e	e	4.4	5.0	0.9
C6	a	c	d	c	b	e	d	a	a	a	d	d	b	b	d	a	a	e	e	d	4.2	5.0	1.2
C7	a	b	d	a	d	c	b	a	c	e	d	e	b	b	d	a	a	e	d	a	4.5	5.0	0.9
C8	e	c	d	b	d	e	b	a	c	c	d	d	b	b	d	a	e	e	e	a	4.2	5.0	1.3
Mean	4.5	3.3	5.0	3.6	4.4	2.0	4.9	4.6	3.9	3.8	4.8	4.5	5.0	4.0	3.9	5.0	4.3	4.9	3.9	4.1			
Median	5.0	3.0	5.0	4.0	4.5	1.0	5.0	5.0	3.5	4.0	5.0	5.0	5.0	4.0	3.5	5.0	5.0	5.0	4.0	5.0			
SD	0.8	0.7	0.0	1.4	0.7	1.5	0.4	1.1	1.0	1.0	0.7	0.9	0.0	0.9	1.0	0.0	1.5	0.4	1.2	1.5			

Table 31 – Computed Confidence Intervals for Test Means

95% Confidence Limits						
Test and Group	Mean	Standard Deviation	Confidence Interval Calculation	Lower Limit	Upper Limit	n
Pre-Training Test for Group A	4.01	1.32	0.914697	3.095	4.925	8
Pre-Training Test for Group B	3.95	1.27	0.880049	3.070	4.830	8
Pre-Training Test for Group C	4.01	1.31	0.907767	3.102	4.918	8
Pre-Training Test for Groups A, B, C	3.99	1.30	0.520099	3.470	4.510	24
Post-Training Test for Group A	4.26	1.56	1.081005	3.179	5.000	8
Post-Training Test for Group B	3.95	1.51	1.046357	2.904	4.996	8
Post-Training Test for Group C	4.21	1.15	0.796895	3.413	5.000	8
Post-Training Test for Group A, B, C	4.14	1.23	0.492093	3.648	4.632	24
Final Test for Group A	4.03	1.30	0.900837	3.129	4.931	8
Final Test for Group B	4.04	1.26	0.873119	3.167	4.913	8
Final Test for Group C	3.98	1.31	0.907767	3.072	4.888	8
Final Test for Group D	3.99	1.35	0.935485	3.055	4.925	8
Final Test for Group A, B, C, D	4.02	1.30	0.450419	3.570	4.470	32
Week 3 Follow-Up A	4.52	0.99	0.686022	3.834	5.000	8
Week 3 Follow-Up B	4.32	1.13	0.783036	3.537	5.000	8
Week 3 Follow-Up A, B	4.42	1.05	0.514491	3.906	4.934	16
Week 6 Follow-Up A	4.22	0.99	0.686022	3.534	4.906	8
Week 6 Follow-Up B	4.18	1.01	0.699881	3.480	4.880	8
Week 6 Follow-Up A, B	4.20	0.99	0.485091	3.715	4.685	16
Week 9 Follow-Up A	4.63	0.99	0.686022	3.944	5.000	8
Week 9 Follow-Up B	4.23	1.18	0.817683	3.412	5.000	8
Week 9 Follow-Up A, B	4.43	1.02	0.817683	3.612	5.000	16

**APPENDIX D: SIMULATED DATA FOR TESTING KRUSKAL-WALLIS
STATISTICAL ANALYSIS**

Below is the sample data used to test the Kruskal-Wallis statistical test. Scores are based on a scale of 1-5, except for Group A the range was from 3-5 for treatment results (assuming that the treatments made a significant difference).

Table 32 – Sample Data for Testing Kruskal-Wallis

Group A Questions	Experimental Group Data range is from 3 - 5										Mean	Median
	1	2	3	4	5	6	7	8	9	10		
1	4	3	4	5	5	5	3	4	5	3	4.00	4.00
2	3	3	3	3	3	3	4	4	4	4	3.50	3.50
3	4	4	5	4	4	4	5	5	5	4	4.20	3.90
4	5	3	4	5	5	4	4	5	4	5	4.20	4.50
5	3	3	3	4	4	4	4	5	3	3	3.70	3.60
6	3	5	3	4	5	4	5	4	3	3	3.90	3.90
7	5	4	3	4	4	4	4	3	5	4	4.10	4.20
8	4	5	5	4	3	5	3	3	5	4	4.00	4.30
9	5	5	5	4	4	4	4	3	3	5	4.20	4.20
10	4	4	4	3	5	4	3	3	4	4	3.90	3.70
Mean:	4.00	4.00	4.00	3.90	4.20	4.10	3.80	3.90	4.00	3.90	4.00	
Median:	3.90	4.00	4.20	3.80	4.10	4.20	3.70	3.80	3.90	3.70		3.90
SD:	0.69	0.73	0.72	0.52	0.56	0.56	0.61	0.66	0.76	0.55	0.62	

Group B Questions	Subject	Control Group									Mean	Median
		1	2	3	4	5	6	7	8	9		
1	4	2	3	5	4	1	1	3	5	2	2.9	2.9
2	5	1	2	5	3	4	2	2	4	3	3.0	2.6
3	1	4	5	2	1	5	3	4	2	4	3.2	3.2
4	3	2	1	3	2	3	2	3	5	1	2.4	2.5
5	3	3	2	2	4	5	3	2	3	3	3.0	3.2
6	2	3	3	5	3	3	4	1	1	4	2.9	3.3
7	5	1	3	3	1	2	2	1	1	2	2.3	2.2
8	2	1	4	3	3	1	3	2	1	4	2.4	2.3
9	4	2	2	3	4	3	1	2	4	2	3.0	2.9
10	4	4	2	2	2	4	5	3	3	1	3.0	2.8
Mean:	3.2	2.5	2.7	3.4	2.7	3.1	2.6	2.4	3.0	2.7	2.82	
Median:	3.3	2.5	2.6	3.0	2.6	3.4	2.6	2.2	3.0	2.4		2.61
SD:	1.230	1.015	1.055	1.102	0.958	1.205	1.185	0.975	1.429	1.142	1.129	

Table 32 – Sample Data for Testing Kruskal-Wallis (cont'd)

Group C Questions	Control Group										Mean	Median
	Subject 1	2	3	4	5	6	7	8	9	10		
1	3	3	5	5	4	2	3	2	2	3	3.3	3.5
2	2	5	1	5	2	2	3	2	4	3	3.0	2.6
3	2	4	3	2	1	1	2	1	2	2	2.0	1.7
4	4	5	5	3	1	3	3	1	3	3	3.2	3.1
5	3	3	4	2	2	4	2	4	2	2	2.9	2.6
6	5	5	2	2	1	4	4	3	4	3	3.3	3.4
7	5	2	4	4	4	2	4	3	3	2	3.3	3.5
8	4	1	2	4	3	5	3	1	5	3	3.2	2.9
9	3	3	1	2	1	1	4	1	3	2	2.2	1.8
10	4	2	2	2	3	3	1	3	3	2	2.6	2.5
Mean:	3.6	3.4	2.9	3.2	2.3	2.7	3.0	2.2	3.1	2.6	2.89	
Median:	3.8	3.4	2.5	2.9	2.4	2.8	3.1	1.9	2.9	2.6		2.84
SD:	1.014	1.290	1.326	1.162	1.104	1.265	1.007	1.063	1.100	0.608	1.144	

Group D Questions	Control Group										Mean	Median
	Subject 1	2	3	4	5	6	7	8	9	10		
1	4	1	3	2	1	1	3	5	5	3	2.8	2.9
2	5	5	4	3	1	4	5	3	1	2	3.3	3.4
3	3	5	1	4	3	3	2	2	1	3	2.7	2.8
4	3	4	4	3	2	2	1	4	3	4	3.1	3.0
5	1	1	1	1	1	1	5	4	4	4	2.4	1.4
6	2	4	3	3	2	1	4	3	3	3	2.9	2.9
7	4	5	1	4	1	2	2	4	1	3	2.7	2.7
8	4	2	4	2	4	2	3	4	3	3	3.0	2.9
9	4	3	3	5	2	5	5	3	2	4	3.5	3.6
10	5	4	4	2	2	1	1	3	1	2	2.6	2.1
Mean:	3.4	3.4	2.9	2.8	2.0	2.3	3.1	3.5	2.4	3.2	2.90	
Median:	3.7	4.0	3.0	2.9	2.0	2.2	2.9	3.5	2.4	3.1		2.96
SD:	1.200	1.469	1.226	1.147	0.855	1.190	1.524	0.868	1.271	0.803	1.225	

Table 33 - Means by Question from Each Group in Simulated Data

Question	Group A	Group B	Group C	Group D
1	4.0	3.2	3.6	3.4
2	4.0	2.5	3.4	3.4
3	4.0	2.7	2.9	2.9
4	3.9	3.4	3.2	2.8
5	4.2	2.7	2.3	2.0
6	4.1	3.1	2.7	2.3
7	3.8	2.6	3.0	3.1
8	3.9	2.4	2.2	3.5
9	4.0	3.0	3.1	2.4
10	3.9	2.7	2.6	3.2
Mean	4.0	2.8	2.9	2.9

Table 34 - Ranking of Means from Simulated Data for Kruskal-Wallis Test

Ranked scores	A	B	C	D	ABCD
For Groups A - D	36.5	23.0	30.0	26.5	Combined
	36.5	7.0	26.5	26.5	
	36.5	11.5	15.5	15.5	
	33.0	26.5	23.0	14.0	
	40.0	11.5	3.5	1.0	
	39.0	20.0	11.5	3.5	
	31.0	8.5	17.5	20.0	
	33.0	5.5	2.0	29.0	
	36.5	17.5	20.0	5.5	
	33.0	11.5	8.5	23.0	
Sum of Ranks	355.0	142.5	158.0	164.5	820.0
Mean of Ranks	35.5	14.3	15.8	16.45	20.5
Number of samples	10	10	10	10	40

*Mean value for each test subject in Groups A, B, C, and D for the post-training test questions (Table 33). The rank ordered scores are for the mean from each test subject in the group (Table 34).

The formula below is for the Kruskal-Wallis test which supposes that there are independent samples of $n_1, n_2 \dots n_k$ observations from K populations. R_1, R_2, \dots, R_k is the sum of the ranks for the K samples when the sample observations are pooled together and ranked in ascending order (Newbold, 2009). The test of the null hypothesis, H_0 , of the equality of the population

means is based on the statistic:
$$W = \frac{12}{n(n+1)} \sum_{i=1}^K \frac{R_i^2}{n_i} - 3(n+1).$$

For the example data above, $W = 22.13817$.
$$W = \frac{12}{40(41)} \left[\frac{(355)^2}{10} + \frac{(142.5)^2}{10} + \frac{(168.5)^2}{10} + \frac{(164.5)^2}{10} \right] - 3(41)$$

We then compare the W value to the value obtained from the Chi-Square distribution function, with $(K-1) = 3$ degrees of freedom with a 5% significance level test, we find that $X_{3,.005}^2$ is equal to 10.60. So our W value is significantly higher, which would mean that we would reject the null hypothesis that the means are the same and would conclude that the training was significant (which we can see from the ranked mean being significantly higher). Lastly, the KW test procedure is approximately valid, provided that the sample contains at least (5) five observations from each sample group (Newbold, 2009).

Table 35 – Simulated data results using PhStat2

Kruskal-Wallis Rank Test for Differences in Medians					
Data					
Level of Significance	0.05	Group	Sample Size	Sum of Ranks	Mean Ranks
		1	10	355	35.5
Intermediate Calculations		2	10	143	14.3
Sum of Squared Ranks/Sample Size	19833.4	3	10	158	15.8
Sum of Sample Sizes	40	4	10	164	16.4
Number of Groups	4				
Test Result					
H Test Statistic	22.12244				
Critical Value	7.814728				
p-Value	6.15E-05				
Reject the null hypothesis					

APPENDIX E: TRAINING SYLLABUS

- A. **Demographic Questions:** The demographic questionnaire consists of 20 multiple choice questions that the subject completes online by accessing the questionnaire via a link that was emailed to them at the beginning of the study period. The demographic questionnaire should not take longer than 10 minutes to complete. Appendix B lists the questions for the demographic questionnaire. Table 36 contains a complete listing of all events and their maximum estimated time.
- B. **Pre-training test:** The pre-training test takes place after the demographic questionnaire. The pre-training test consists of 20 questions presented in a multiple choice format. The test is to determine the level of knowledge that each subject has in the area of computer security, particularly as it relates to an online environment. The pre-training test should not take more than 20-30 minutes to complete (see Appendix B). The pilot study helped to determine the actual time that will be needed to complete the pre-training test.
- C. **Initial training with simulated scenarios:** The initial training with simulated scenarios took place 1 - 2 weeks after the pre-training test. The initial training consists of security information presented to the subject about the major areas of information and computer security. Included were simulated events on emails, social engineering, phishing and file sharing. Approximately 20 simulated events were presented and took approximately 30-45 minutes to complete. After the training, a post-training test of 10 questions was provided to test the subject on the material presented in the initial training with simulated scenarios. The post-training

test takes approximately 10-15 minutes to complete and contains questions that are similar in content to the pre-training test to see if the subjects' awareness of security improved based on training and testing. Appendix F provides some examples of the simulated events. The following information is a draft of the subjects' training.

- a. A definition of computer security is presented to the subjects along with a list of terms that are commonly used in computer security to provide a baseline of knowledge. Included are simulated events that show how security is normally breached – such as a user opening an email attachment from an unknown sender, and a user providing information to another user that they do not check their identity, etc.
- b. Next, the subjects are provided with examples of organizations that have been breached by hackers due to routine carelessness on the part of end-users of the information system. Examples are listed in Chapter 2. The information is presented in such a way that users are made aware of the importance of maintaining security of their system and in their V-CoP environment. The data is presented in an online format and includes simulated events that show how some of the breaches are done. Here are some examples:
 - i. In a study conducted by the McAfee Corporation, it is projected that companies worldwide lost more than \$1 trillion to computer security breaches in 2008 alone. Also, Forrester Research estimates that an

average computer security breach can cost a company between \$90 and \$305 per record. Since most breaches do not just involve tens or even hundreds of records, but rather hundreds of thousands or even millions of records, the cost of the breach and the cost of repair can be in the millions of dollars. For example, TJX Companies Inc. was hacked in 2007 and a reported 46 to 215 million customer records were stolen. The cost to TJX could theoretically be as high as \$65 billion (215 million records at \$305 per record). Questions arise about the causes and remedies of these breaches. In this virtual world of computer transactions, how does an organization adequately protect its valuable information assets? The importance of proper security procedures and adhering to those procedures is a critical component to any system.

- ii. Insider breaches are a major concern of organizations. A temporary telecom company employee was arrested on charges of stealing personal information and then pocketing more than \$70,000 by taking out short-term payday loans. Even one of the world's leading anti-virus and internet security providers had an international office employee steal customers' credit card numbers. Insider breaches will continue to be a rising threat for 2010 and beyond, as long as companies do not have the proper policies in place to prevent them.

- iii. 160,000 California university records were hacked at one of California's most esteemed universities. Personal information of 160,000 current and former students and alumni may have been compromised. These students and alumni are now vulnerable to identity theft and other illegal hacking activities.
- iv. Weak passwords are those passwords that are quickly hacked by software hacking tools or by good guessing. One of the easiest ways for hackers to gain access to confidential data is through password cracking. For example, an 18-year-old student performed a password attack on Twitter by writing a program to do a rapid-fire dictionary log-on for the user Crystal, whose name he found frequently in Twitter feeds. He thought she was just popular, but in fact she was a Twitter staffer. When he got into her account, which had the weak password "happiness," he had access to the administrative control panel for Twitter, and could change anyone's password. From there it was off to the races. The use of "weak" passwords is unfortunately common and very dangerous. Once a hacker gains access to a system, particularly through an account that has administrative (or all) privileges, they essentially have access to everything on the remote system. In an online community, this means they can delete

accounts, download sensitive data, create new accounts, take down the system, delete everything, and more.

D. Simulated Security Training and Testing: Approximately 3, 6, and 9 weeks after the initial training with simulated scenarios event, follow up simulated security training and testing takes place. Subjects involved in this phase (Groups A and B) receive another email telling them where to go to complete the brief training and testing. Approximately 10 simulated scenarios with questions are included in this phase of the research. The event takes approximately 20 minutes to complete. See Appendix F for examples of the training and testing. An example is listed below.

- a. The subject is presented with the following screen, and will have to change their password using a password that they believe is a strong password. The system then displays their password, and asks if it is strong in context of the definition, which is displayed with their password. They then have to answer a question that lists a group of passwords and they are to select the password they believe to be appropriate based on strength of the password and usability.

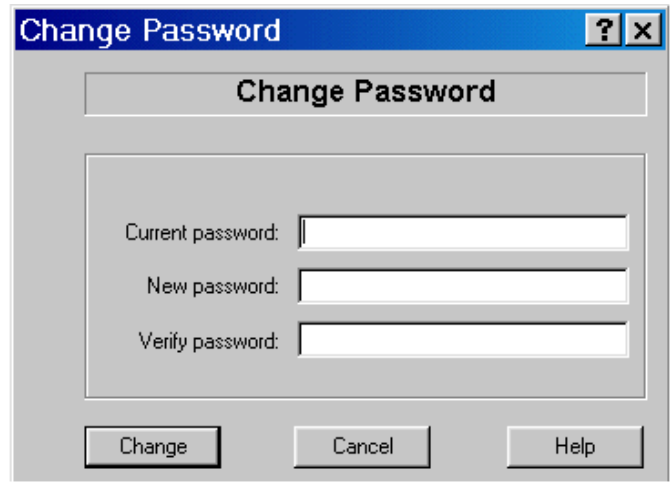


Figure 42 – Simulated Example Event

- E. **Final Test and Interview:** Approximately 10 weeks after the initial training with simulated scenarios, and after the last simulated security training and testing event, a final test is performed on all groups to measure the learning from the training and testing, or from the pre-training test alone. The final test takes approximately 15-20 minutes to complete. Interviews might have been conducted if certain subjects have skewed responses or scores. The interviews would have been done over the phone or via email.

Table 36 - Maximum Estimated Training with simulated scenarios and Testing Time

Event	Maximum Estimated Time in Minutes for Each Event			
	Group A	Group B	Group C	Group D
Demographic Questionnaire	15	15	15	15
Pre-Training Test	20	20	20	
Initial Training	30		30	
Post-Training Test	20	20	20	
4 th Week Simulated security testing and training	30	30		
7 th Week Simulated security testing and training	30	30		
10 th Week Simulated security testing and training	30	30		
Final Test And Interviews	20	20	20	20
Total Estimated Time for All Events	195 min	165 min	105 min	35 min

APPENDIX F: SAMPLES OF TRAINING WITH SIMULATED SCENARIOS AND TESTING EVENTS

Sample of Training with simulated scenarios and Testing

1. The subject is presented with a simulated (web interface) email message with an attached file named Information.zip. The email message states that the file is information that they requested from another member of the V-CoP. The email appears to be from a legitimate member of the V-CoP and the return email address seems valid. Attempts will be made to get the subject to click on the file attachment. If they click on the file attachment they will get a simulated error message stating that they have been infected by a virus. Immediately after their response, they will be presented with a multiple choice question asking them about the most secure way to respond to the previous email attachment simulation.

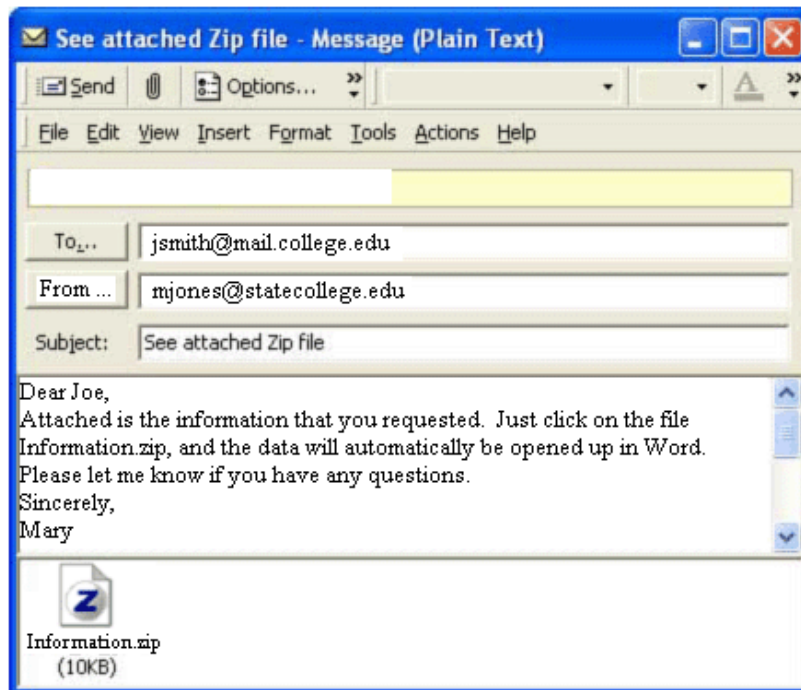


Figure 43 – Sample Email Simulated Event

2. The subject is presented with a link to a recorded voice message that asks them to provide their username and password to the IT department. The IT staff person, Susan, says that they are testing the network and need to verify the data packets traveling across the network. The subject is asked to respond to the simulated “person’s voice” by answering a question on what information they should provide to Susan. Here is what the voice would say: “Hey Joe, this is Susan from the technology department on campus. We are testing the network and we need to make sure that the data we are verifying is from your computer. I know that your user name is jsmith, and you are using what password with your account? Once we check the network we will reset your password and email you your new password. This should only take a couple of minutes. Thanks again. We really appreciate your help Susan.”

3. The next simulation will be of a list of files that are posted to the V-CoP site. One of the files is a Pilot-Test.ZIP file that was posted by an apparent member of the V-CoP and has a note next to it stating “Results from chemistry pre-training test pilot program”. The members have been working on this and are looking forward to seeing if the pre-training test for student self-assessment was effective. The file was actually uploaded by someone who hacked into the V-CoP and placed the file there after reading about the project for the chemistry pre-training test pilot program. If the user clicks on the file, it will state that it is a virus and their computer has been

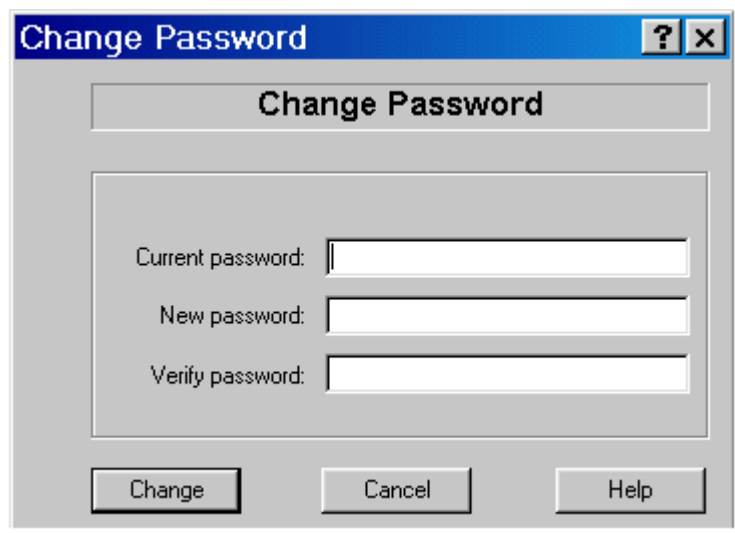
infected. They will then be immediately asked a question about what they should do next to solve the problem, based on the most secure response.

The screenshot shows a web interface for 'Curriculum Alignment: Chemistry'. At the top right, there is a search bar with 'This Site' selected. The main content is organized into several sections:

- Blogs:** A table with columns for Title, Created By, Published, Category, # Comments, and Edit. Below the table is a link to 'Add a new item'.
- Working Documents:** A table with columns for Type, Name, Modified, and Modified By. It lists several documents such as '200840 CHM 1045 Syllabus' and 'CHM 1046 Exam 1 CA 365760'. Below the table is a link to 'Add new document'.
- Course Placement Exams:** A table with columns for Type, Name, and Modified By. It lists one document: 'Pilot-Test NEW'. Below the table is a link to 'Add new document'.
- Project Administration:** A section with a dropdown arrow and a list of items: 'Meeting Agendas', 'Meeting Summaries', and 'Upcoming Activities'. Below the list is a link to 'Add new document'.
- Calendar of Events:** A section with a dropdown arrow and a message: 'There are currently no upcoming events. To add a new event, click "Add new event" below.' Below the message is a link to 'Add new event'.
- Participants:** A section with a dropdown arrow and a list of names: Allison, Anthor, Barbar, Bob Ke, Carol H, Charler, Claude, Clifton, Craig T, Cristine, Daeri T, Dave H, Debora, and Don As.

Figure 44 – Sample Potential Virus File

4. Another simulation would be related to password security. The subject would be prompted to change their password. After they enter their new password, they would be presented with a question that asks them to identify the strongest password from a choice of five alternatives. The password they entered will be presented to them and they can compare their selection with the choices in the question.



The image shows a standard Windows-style dialog box titled "Change Password". The title bar is blue and contains the text "Change Password" along with a question mark icon and a close button (X). The main area of the dialog is grey and contains a title bar with the text "Change Password". Below this, there are three text input fields labeled "Current password:", "New password:", and "Verify password:". At the bottom of the dialog, there are three buttons: "Change", "Cancel", and "Help".

Figure 45 – Sample Password Simulation

APPENDIX G: POTENTIAL INTERVIEW QUESTIONS

Potential Interview Questions

Note: Interviews of some subjects would have been conducted based on irregularities or skewed responses from a particular test subject or targeted at the treatment group to get further feedback on the effectiveness of the training with simulated scenarios and how it would affect their future behavior. Some example interview questions were developed and include the following.

1. How did the computer security training change your perception of sharing data in a virtual community?
2. How would you rate your awareness of computer security before and after your involvement in this research?
3. Even though you did not receive pre-training in computer security your responses to the pre – and post-training test were different. What would you attribute this change in responses?
4. What changes would you recommend to the training that you received in the initial training event, and the subsequent intermittent events at 3, 6, and 9 weeks?
5. Were the questions and training events easy to understand and apply? Why or why not?
6. How will you change, if any, your behaviors as it relates to computer security in your organization?
7. What changes do you think need to be made to the security awareness policies at your organization?
8. Would you recommend this training to others at your organization? Why or why not?
9. In what ways can your organization better serve its employees in the area of information security and awareness?
10. Are there any other comments or suggestions that you have about this training system?

APPENDIX H: IRB INFORMED CONSENT



**Measuring the Effect of Using Simulated Security Awareness Training and Testing on
Members of Virtual Communities of Practice.
Informed Consent**

Principal Investigator(s): Craig L. Tidwell, Doctoral Student

Sub-Investigator(s): N/A

Faculty Supervisor: Charles Reilly, PhD

Investigational Site(s): Online, via the Internet

Introduction: Researchers at the University of Central Florida (UCF) study many topics. To do this we need the help of people who agree to take part in a research study. You are being invited to take part in a research study which will include about 20-40 people from UCF. You have been asked to take part in this research study because you are a teacher and are involved in a virtual community of practice (Curriculum Alignment group). You must be 18 years of age or older to be included in the research study.

The person doing this research is Craig L. Tidwell of UCF College of Engineering and Computer Science, Modeling and Simulation PhD program. Because the researcher is a graduate student, he is being guided by Dr. Charles Reilly, a UCF faculty supervisor in the College of Engineering and Computer Science.

What you should know about a research study:

- Someone will explain this research study to you.
- A research study is something you volunteer for.
- Whether or not you take part is up to you.
- You should take part in this study only because you want to.
- You can choose not to take part in the research study.
- You can agree to take part now and later change your mind.
- Whatever you decide it will not be held against you.
- Feel free to ask all the questions you want before you decide.

University of Central Florida IRB
IRB NUMBER: SBE-10-06708
IRB APPROVAL DATE: 3/23/2010
IRB EXPIRATION DATE: 3/22/2011

Purpose of the research study: The purpose of this study is to measure the effect of simulated web-based training and testing on information security awareness over a 12 week period.

What you will be asked to do in the study: You will be randomly assigned (like the flip of a coin) to 1 of 4 groups. Your selection will be random based on the total number of participants, equally distributed between the 4 groups to create groups of equal size.

You will be asked to take part in the research by answering questions related to information security. Depending on the group you are assigned to, you may be asked to take information security training with simulated scenarios at specified intervals, take a pre and post-training test to measure the effect of the simulated information security training and testing, and respond to possible interview questions at the end of the study. Each segment of the study should not take more than 30 minutes to complete.

Time Frame	Group A	Group B	Group C	Group D
Start	Demographic Questionnaire	Demographic Questionnaire	Demographic Questionnaire	Demographic Questionnaire
Start	Pre-training test	Pre-training test	Pre-training test	
1-2 weeks	Simulated Security Awareness Training and Post-training test	Post-training test	Simulated Security Awareness Training and Post-training test	
3 weeks	Simulated Security Testing and Training	Simulated Security Testing and Training		
6 weeks	Simulated Security Testing and Training	Simulated Security Testing and Training		
9 weeks	Simulated Security Testing and Training	Simulated Security Testing and Training		
10 weeks	Final Test (Interviews)	Final Test (Interviews)	Final Test (Interviews)	Final Test (Interviews)

Below is the table of events and then a table of time for each event:

Event	Maximum Estimated Time in Minutes for Each Event			
	Group A	Group B	Group C	Group D
Demographic Questionnaire	15	15	15	15
Pre-training test	20	20	20	
Initial Training	30		30	
Post-training test	20	20	20	
4 th Week Simulated security testing and training	30	30		
7 th Week Simulated security testing and training	30	30		
10 th Week Simulated security testing and training	30	30		
Final Test And Interviews	20	20	20	20
Total Estimated Time for All Events	195 min	165 min	105 min	35 min

You do not have to answer every question or complete every task. You will not lose any benefits if you skip questions or tasks.

Location: The entire research will be conducted online in a web-based environment. Participants in the study will be given a sign-on number and password to take part in the study at its start.

Time required: There will be a maximum of 5 online sessions that will last approximately 30 minutes over the 12 week period. All sessions will be done online through the Internet.

Audio or video taping: This study does not include any audio or video taping.

Risks: There are no expected risks for taking part in this study. You do not have to answer every question or complete every task. You will not lose any benefits if you skip questions or tasks. You do not have to answer any questions that make you feel uncomfortable.

Benefits: You may benefit from this research. You may become more aware of information security risks and procedures for dealing with these risks.

University of Central Florida IRB
 IRB NUMBER: SBE-10-06708
 IRB APPROVAL DATE: 3/23/2010
 IRB EXPIRATION DATE: 3/22/2011

Compensation or payment: There is no compensation or other payment to you for taking part in this study. There is no compensation, payment or extra credit for taking part in this study.

It is possible, however, that if you are a student involved in the pilot study, you may earn extra credit for your participation, but this benefit is at the discretion of the instructor. If you choose not to participate, you may notify your instructor and ask for an alternative assignment of equal effort for equal credit. There will be no penalty for not participating.

Confidentiality: Your identity will be kept confidential. The researcher will make every effort to prevent anyone who is not on the research team from knowing that you gave us information, or what that information is. For example, your name will be kept separate from the information you give, and these two things will be stored in different places.

Your information will be combined with information from other people who took part in this study. When the researcher writes about this study to share what was learned with other researchers, he will write about this combined information. Your name will not be used in any report, so people will not know how you answered or what you did.

Study contact for questions about the study or to report a problem: If you have questions, concerns, or complaints, or think the research has hurt you, talk to Craig L. Tidwell, Doctoral Graduate Student, Modeling and Simulation, College of Engineering and Computer Science, (407) 221-2073 or Dr. Charles Reilly, Faculty Supervisor, Department of Industrial Engineering and Management Systems at (407) 823-5306 or by email at creily@mail.ucf.edu.

IRB contact about your rights in the study or to report a complaint: Research at the University of Central Florida involving human participants is carried out under the oversight of the Institutional Review Board (UCF IRB). This research has been reviewed and approved by the IRB. For information about the rights of people who take part in research, please contact: Institutional Review Board, University of Central Florida, Office of Research & Commercialization, 12201 Research Parkway, Suite 501, Orlando, FL 32826-3246 or by telephone at (407) 823-2901. You may also talk to them for any of the following:

- Your questions, concerns, or complaints are not being answered by the research team.
- You cannot reach the research team.
- You want to talk to someone besides the research team.
- You want to get information or provide input about this research.

University of Central Florida IRB
IRB NUMBER: SBE-10-06708
IRB APPROVAL DATE: 3/23/2010
IRB EXPIRATION DATE: 3/22/2011

Withdrawing from the study: If you decide to leave the research, data will not be made available to complete the research study and will impact the final results. If you decide to leave the study, contact the investigator so that the investigator can make sure that you are removed from the pool of subjects. The person in charge of the research study or the sponsor can remove you from the research study without your approval. The sponsor can also end the research study early. We will tell you about any new information that may affect your health, welfare or choice to stay in the research.

LIST OF REFERENCES

- Adhikari, R. (2009): "Study: Negligence Causes Most Data Breaches." Internet News.Com. Retrieved from the world wide web at <http://www.internetnews.com/business/article.php/3800026>.
- Anderson, R. (1996): "A Security Policy Model for Clinical Information Systems." IEEE Symposium on Security and Privacy, 1996.
- Ardichvili, A., Page, V., & Wentling, T. (2003): "Motivation and barriers to participation in virtual knowledge-sharing communities of practice." *Journal of Knowledge Management*, Vol. 7, No. 1, 2003, pp. 64-77.
- Aslam, T., Krsul, I., & Spafford, E. (1996): "Use of a Taxonomy of Security Faults." 19th National Information Systems Security Conference, October 22-25, 1996, Baltimore, MD.
- Baker, W., Hylender, C., & Walentine, J. (2008): "2008 Data Breach Investigations Report: A study conducted by the Verizon Business RISK Team." Retrieved from the World Wide Web at <http://www.verizonbusiness.com/resources/security/databreachreport.pdf> pp. 1-27 on December 10, 2008.
- Barth, S. (2004): "Three thousand communities of practice.", *KM World* (Vol. 13, pp. 20): Information Today Inc.
- Bell, David (2005): "Looking Back at the Bell-La Padula Model." ACSAC (Annual Computer Security Applications Conference) 2005 proceedings of the 21st ACSAC, Tucson, AZ. IEEE Xplore.
- Besnard, D., & Arief, B. (2004): "Computer Security Impaired by Legitimate Users." *Computers & Society*, vol. 23, pp. 253-264.
- Bieber, et al. (2002): "Towards Knowledge-Sharing and Learning in Virtual Professional Communities." Proceedings of the 35th Hawaii International Conference on System Sciences, 2002.
- Bishop, M. (2003): "What is Computer Security?" *IEEE Security & Privacy*, Jan/Feb 2003, pp. 67-69.

- Blake, S. (2000): "The Clark-Wilson Security Model." Indiana University of Pennsylvania, Library Resources. Retrieved from the World Wide Web at <http://www.lib.iup.edu/comscisec/SANSpapers/blake.htm>, on January 10, 2009.
- Boella, G., & van der Torre, L. (2006): "Security Policies for Sharing Knowledge in Virtual Communities." IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans. Vol. 36, No. 3, pp. 439-450, May 2006.
- Chang, S., Qiming, C., & Hsu, M. (2003): "Managing Security Policy in a Large Distributed Web Services Environment." Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC '03). pp. 610-621. Dallas, TX.
- Cholvy, L., & Cuppens, F. (1997): "Analyzing Consistency of Security Policies." IEEE Symposium on Security and Privacy, pp. 1-10. Oakland, CA.
- Coakes, E., & Clarke, S. (2005, October): "Encyclopedia of Communities of Practice in Information and Knowledge Management." Idea Group Publishing.
- Cuppens, F., Cuppens-Boulahia, N., Sans, T., & Mieke, A. (2005): "A formal approach to specify and deploy a network security policy." IFIP International Federation for Information Processing, Vol. 173, pp. 203-218.
- Cuppens, F., & Saurel, C. (1996): "Specifying a Security Policy: A Case Study." Computer Security Foundations Workshop, 1996. Proceedings., Ninth IEEE Computer Security Foundations Workshop. pp.123-134.
- Damm, D., & Schindler, M. (2002): "Security issues of a knowledge medium for distributed project work." International Journal of Project Management, Vol 20, pp. 37-47.
- Davies, J., Duke, A., & Sure, Y. (2003): "OntoShare – A Knowledge Management Environment for Virtual Communities of Practice." International Conference on Knowledge Capture, Proceedings of the 2nd international conference on Knowledge capture pp. 20-27.
- Denning, D. (1976): "The Lattice Model of Secure Information Flow." Communications of the ACM, vol. 19, no 5, pp. 236-242.
- Dhillon G., & Backhouse J. (2001): "Current directions in IS security research: towards socio-organizational perspectives." Information Systems Journal, Volume 11, Number 2, April 2001, pp. 127-153(27)

- Dickinson, J. (2005): "The New Anti-Virus Formula: How to Use Multilayered Security to Defeat Viruses." Messaging News Press, www.messagingnews.com, retrieved Aug 24, 2009 from the World Wide Web.
- Dobson, J., & McDermid, J. (1989): "A framework for expressing models of security policy." Proceedings, 1989 IEEE Symposium on Security and Privacy. pp. 229-239.
- Dunning, D., Gathercole, S, & Holmes, J. (2009): "Adaptive training leads to sustained enhancement of poor working memory in children." *Developmental Science*, vol. 12, no 4, July 2009
- Epstein, K., & Elgin, B. (2008): "Network Security Breaches Plague NASA." *Business Week Online* – http://www.businessweek.com/magazine/content/08_48.
- Faraj, S., & Wasko, M.M. (2001): "The Web of Knowledge: An Investigation of Knowledge Exchange in Networks of Practice." Cambridge, MA: Open Source Research Community and MIT.
- Gaudin, S. (2007): "Security Breaches Cost \$90 To \$305 Per Lost Record." *Information Week*. Retrieved from the World Wide Web at <http://informationweek.com/story/showarticle.jhtml?articleid=199000222> on January 12, 2009.
- Gongla, P. & Rizzuto, C.R. (2001): "Evolving communities of practice: IBM Global Services experience." *IBM Systems Journal*, 40(4), 842-862.
- Greenemeier, L. (2008): "Security Breach: Feds Lose Laptop Containing Sensitive Data – Again." *Scientific American*, March 2008.
- Gritzalis, Z. & Lambrinoudakis, C. (2004): "A security architecture for interconnecting health information systems." *International Journal of Medical Informatics* (2004), 73, pp. 305-309.
- Hakala, D. (2008): "The Worst IT Security Breaches of 2007." *IT Security.com*. Retrieved from the World Wide Web at <http://www.itsecurity.com/features/top-security-breaches-2007-012208/> on March 12, 2009.
- Hamed, H., & Al-Shaer, E. (2006): "Taxonomy of Conflicts in Network Security Policies." *IEEE Communications Magazine*, March 2006, pp 134-141.

- Handley, K., Sturdy, A., Fincham, R., & Clark, T. (2006): "Within and Beyond Communities of Practice: Making Sense of Learning Through Participation, Identify and Practice." *Journal of Management Studies*, Vol. 43, May 2006.
- Higgins, G. (2005): "An Application of Deterrence Theory to Software Piracy." *Journal of Criminal Justice and Popular Culture*, 12 (3), 166-184. 2005
- Hung, D., Chee, T., Hedberg, J., & Seng, K. (2005): "A framework for fostering a community of practice: scaffolding learners through an evolving continuum." *British Journal of Educational Technology*. Vol. 36, No. 2. pp. 159-176.
- Johnson, C. (2001): "A survey of current research on online communities of practice." *Internet and Higher Education* 4, pp. 45-60.
- Johnson, E., & Khalidi, R. (2005): "Communities of practice for development in the Middle East and North Africa." *KM4D Journal* 1(1): p90-103.
- Kimble, C., Feng, L., & Barlow, A. (2000): "Effective Virtual Teams Through Communities of Practice." *Management Science - Theory, Method & Practice*. Social Science Research Network.
- Kjaerland, M. (2006): "A taxonomy and comparison of computer security incidents from the commercial and government sectors." *Computers & Security*, 2006. Pp 522-538
- Knights, M. (2009): "Security breaches cost \$1 trillion last year." *ITPro*, January 29, 2009. Retrieved from the web at <http://www.itpro.co.uk/609689/security-breaches-cost-1-trillion-last-year>, on April 12, 2009.
- Lampson, B. (2000): "Computer Security in the Real World." *Annual Computer Security Applications Conference*, 2000, pp 37-46.
- Lesser, E. L., & Storck, J. (2001): "Communities of practice and organizational performance." *IBM Systems Journal*, Vol. 4, No. 4. 2001.
- Liu, F., & Koenig, H. (2008): "Security Policy Management for peer Group Meetings." *Emerging Security Information, Systems and Technologies*, 2008. SECURWARE '08. Second International Conference, August 25-31, 2008 - Cap Esterel, France.
- Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, Vol. 16, No. 2, pp. 173-186.

- Loyarte, E., & Rivera, O. (2007): "Communities of practice: a model for their cultivation." *Journal of Knowledge Management*, Vol. 11, No. 3, pp. 67-77.
- Lueg, C. (2000): "Where is the Action in Virtual Communities of Practice?" *Proceedings of D-CSCW – German Conference on Computer Supported Cooperative Work*.
- McGlasson, L. (2008): "Top 10 Security Breaches of 2008." *Bank Info Security Online*. Retrieved from the World Wide Web at http://www.bankinfosecurity.com/articles.php?art_id=1139 on February 15, 2009.
- Merali, Y., & Davies, J. (2001): "Knowledge Capture and Utilization in Virtual Communities." *Proceedings of the 1st international conference on Knowledge capture*, Victoria, British Columbia, Canada. ACM Special Interest Group on Artificial Intelligence. pp. 92-99.
- Muthaiyah, S., & Kerschberg, L. (2007): "Virtual organization security policies: An ontology-based integration approach." *Inf Syst Front*, Vol. 9, pp. 505–514, Springer Science.
- Nautilus Institute (1995): "Essentials of Post-Cold War Deterrence." Retrieved from the World Wide Web at <http://www.nautilus.org/archives/nukestrat/USA/Advisory/essentials95.PDF> on April 10, 2009.
- Neus, A. (2001): "Managing Information Quality in Virtual Communities of Practice." *IQ*, 2001 - opensource.mit.edu
- Newbold, P., Carlson, W., & Thorne, B. (2009): "Statistics for Business and Economics." Seventh Edition, Prentice Hall Publishers, ISBN# 978-0-13-608536-2.
- Norman, P.M. (2002): "Protecting knowledge in strategic alliances: Resource and relational characteristics." *Journal of High Technology Management Research*, 12, 177-202.
- Pearlman, Welch, Foster, Kesselman, and Tuecke (2002): "A community authorization service for group collaboration," in *Proc. IEEE Int. Workshop Policies Distributed Systems and Networks*, 2002, pp. 50–59.
- Ramaswamy, R., Storer, G., & Romeck, V. (2005): "Designing sustainable communities of practice at CARE." *Knowledge Management for Development Journal*, Vol. 1, No. 1, pp. 76-89.

- Richardson, R. (2008): "2008 CSI Computer Crime & Security Survey." Retrieved from the web at <http://i.cmpnet.com/v2.gocsi.com> pp 1-30.
- Roberts, J. (2006): "Limits to Communities of Practice." *Journal of Management Studies*, Vol. 43, No 3.
- Rosencrance, L. (2005): "Kaiser Permanente patient data exposed online." *Computerworld Security*, March 16, 2005. Retrieved from the World Wide Web at http://www.computerworld.com/s/article/100420/Update_Kaiser_Permanente_patient_data_exposed_online_on_January_21, 2009.
- Sans.org (2005): "Mistakes People Make that Lead to Security Breaches." Retrieved from the World Wide Web at <http://www.sans.org/resources/mistakes.php?ref=3816> on February 17, 2009.
- Sans.org (2009): "The SANS Security Policy Project." From www.sans.org. Retrieved from the World Wide Web at <http://www.sans.org/resources/policies/#name>. on May 15, 2009.
- Saravanan, M., & Kerschberg, L. (2007): "Virtual organization security policies: An ontology-based integration approach." *Information Systems Frontiers*, Vol. 9, No 5, pp. 505-514.
- Schneider, F. (2003): "Enforceable Security Policies." *Proceedings of the Foundations of Intrusion Tolerant Systems (OASIS'03)*.
- Sharratt, M., & Usoro, A. (2003): "Understanding Knowledge-Sharing in Online Communities of Practice." *Electronic Journal on Knowledge Management*, Vol. 1, No. 2, pp. 187-196.
- Siponen, M., & Oinas-Kukkonen, H. (2007): "A Review of Information Security Issues and Respective Research Contributions." *The Database for Advances in Information Systems*. Vol. 38, No 1, pp. 60-80.
- Sloman, M. (1994): "Policy driven management of distributed systems," *Journal of network and Systems Management*, Vol. 2, No. 4, pp. 333-360.
- Steinfeld, C., Jang, C., & Pfaff, B. (1999): "Supporting Virtual Team Collaboration: The TeamSCOPE System." *Conference on Supporting Group Work, Proceedings of the international ACM SIGGROUP conference on supporting group work*. Phoenix, AZ. pp. 81-90.

- Straub, D. & Welke, R. (1998): "Coping with Systems Risk: Security Planning Models for Management Decision Making." *MIS Quarterly*, Vol. 22, No. 4. pp. 441-469.
- Summers, C. Rita (1997): "Computer Security: Threats and Safeguards." McGraw Hill, New York.
- van Elst, L., Dignum, V., and Abecker, A. (2004): "Towards agent-mediated knowledge management," in *Proc. Agent-Mediated Knowledge Management*, vol. 2926. Berlin, Germany: Springer-Verlag, 2004, pp. 1-30.
- Von Solms, B., & Von Solms, R. (2004): "The 10 deadly sins of information security management." *Computers and Security*, 23, pp 371-376.
- Walker, D. (2007): "U.Va. reports computer security breach." Associated Press. Retrieved from the World Wide Web at <http://www.msnbc.msn.com/id/19121652> on May 10, 2009.
- Wasko, M., & Faraj, S. (2000): "It is what one does': why people participate and help others in electronic communities of practice." *The Journal of Strategic Information Systems*, Vol. 9 Nos. 2-3, pp. 55-173.
- Wasko, M., & Faraj, S. (2005): "Why should I share? Examining Social Capital and Knowledge Contribution in Electronic Networks of Practice." *MIS Quarterly*, Vol. 29 No. 1, pp. 35-57/March 2005.
- Wenger, E. (1999): "Communities of practice: learning, meaning, and identity." Cambridge University Press; 1st edition.
- Wenger, E. (2000): "Communities of Practice and Social Learning Systems." Sage Publications, Vol. 7(2): pp. 225-246.
- Wenger, E. (2004): "Knowledge management as a doughnut: Shaping your knowledge strategy through communities of practice." *Ivey Business Journal*, Jan-Feb 2004.
- Wenger, E., McDermott, R., & Snyder, W.M. (2002): "Cultivating communities of practice: A guide to managing knowledge." Boston: Harvard Business School Press.
- Wenger, E. & Snyder, W. (2000): "Communities of Practice: The Organizational Frontier." *Harvard Business Review*, Jan-Feb 2000.

- Whitman, M. (2004): "In defense of the realm: understanding the threats to information security." *International Journal of Information Management*, Vol 24, pp. 43-57.
- Whitman, M, Townsend, A.M., & Hendrickson, A.R. (1999). Cross-national differences in computer-use ethics: A nine country study. *The Journal of International Business Studies*, Vol. 30, No. 4, pp. 673–687.
- Wilson, L. (2009): "Facing the Information Security Hole in 2009." Retrieved from the World Wide Web at <http://www.Information-Security-Resources.com> on February 2, 2009.
- Yampolskiy, R., & Govindaraju, V. (2007): "Computer Security: a Survey of Methods and Systems." *Journal of Computer Science*, Vol. 3, No. 7, pp. 478-486.
- Zhang, W., & Watts, S. (2008): "Online communities as communities of practice: a case study." *Journal of Knowledge Management*, Vol. 12, No. 4, pp. 55-71.