



**THE EFFECT OF INTERACTIVITY AND INSTRUCTIONAL
EXPOSURE ON LEARNING EFFECTIVENESS AND
KNOWLEDGE RETENTION: A COMPARATIVE STUDY OF
TWO U.S. AIR FORCE COMPUTER-BASED TRAINING (CBT)
COURSES FOR NETWORK USER LICENSING**

THESIS

Matthew J. Imperial, Captain, USAF

AFIT/GIR/ENV/03-07

**DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY**

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/03-07

THE EFFECT OF INTERACTIVITY AND INSTRUCTIONAL EXPOSURE ON
LEARNING EFFECTIVENESS AND KNOWLEDGE RETENTION:
A COMPARATIVE STUDY OF TWO U.S. AIR FORCE COMPUTER-BASED
TRAINING (CBT) COURSES FOR NETWORK USER LICENSING

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the
Degree of Master of Science in Information Systems Management

Matthew J. Imperial, BS

Captain, USAF

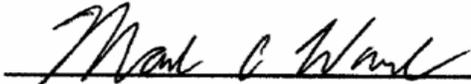
March 2003

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

THE EFFECT OF INTERACTIVITY AND INSTRUCTIONAL EXPOSURE ON
LEARNING EFFECTIVENESS AND KNOWLEDGE RETENTION:
A COMPARATIVE STUDY OF TWO U.S. AIR FORCE COMPUTER-BASED
TRAINING (CBT) COURSES FOR NETWORK USER LICENSING

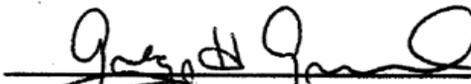
Matthew J. Imperial, BS
Captain, USAF

Approved:



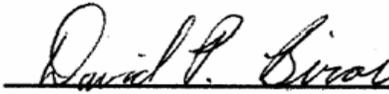
Mark A. Ward, Major, USAF (Chairman)

3 March 2003
date



Gregg H. Gunsch, PhD (Member)

3 March 2003
date



David P. Biros, Lieutenant Colonel, USAF (Member)

3 March 2003
date

Acknowledgments

"I can do all things through Christ who strengthens me" (Philippians 4:13)

This long, difficult, and rewarding process of graduate school has now come to fruition and as such there are many individuals to thank for aiding my journey along the way. I would first like to thank my amazing wife for her love, support, and unyielding devotion throughout my degree program. Her ability to pursue her own doctoral degree while still driving me towards excellence is awe-inspiring. Many a late nights were spent by Team Imperial in the AFIT computer lab.

I would like to thank my thesis committee members: my advisor Major Ward for his advice, patience, and guidance; and my two readers Dr. Gunsch and Lieutenant Colonel Biros for their scrutiny in helping me produce a refined research product.

I also owe a large debt of gratitude to Mr. Maddin and Mr. Stamper from AFIT/SC. Their technical support was invaluable, their tolerance for change appreciated, and their customer service was truly second to none.

I'd also like to acknowledge my fellow classmates of GIR 03M. Thanks to each of you who helped support thesis research efforts, class studies, and social occasions not to be forgotten.

The Air Force, the United States, and the world have seen dramatic changes during my program here at AFIT. As my pursuit of a graduate degree draws to conclusion, I am reminded that our freedom is precious and our willingness to defend that freedom uncompromising.

Matthew J. Imperial

Table of Contents

	Page
Acknowledgments.....	iv
List of Figures.....	viii
List of Tables.....	ix
List of Equations.....	xi
Abstract.....	xii
I. Introduction.....	1
Background.....	1
Benefits and Costs of CBT.....	2
Military Use of CBT.....	3
Information Assurance Training.....	5
Information Assurance Training in a CBT Domain and Beyond.....	6
Problem Statement - Research Questions.....	8
Scope.....	10
Contribution to Researchers and Practitioners.....	11
Summary.....	12
II. Literature Review.....	14
Overview.....	14
Learning Theories and Teaching Strategies.....	14
Learning Theories and CBT.....	15
Sociocultural Theory of Learning.....	16
Constructivist Theory of Learning.....	17
Sociocultural and Constructivist Learning Theories.....	18
Teaching Strategies and CBT.....	18
Individualized Instruction.....	19
Interactivity.....	19
Human Perception.....	22
Programmed Instruction.....	24
Learning Theories and Teaching Strategies Summary.....	25
Learning Effectiveness and CBT.....	26
Knowledge Retention.....	28
Overview of an Online CBT Program.....	30
AFCA NUL CBT.....	31
WPAFB USC/WIAT CBT.....	33

	Page
NUL and USC/WIAT Objectives and Exams	34
Training Domains and Mediums	34
Information Assurance Education, Training, and Awareness (IA ETA)	35
Awareness	36
Training	37
Education	39
Job Field and Other Demographics	41
Hypotheses	43
Summary	44
 III. Methodology	 45
Overview	45
Research Methodology	46
Interactivity Content Analysis, NUL and USC/WIAT	47
Quasi-experimental component	48
Survey component	51
Pilot Study	53
Population	53
Subjects	54
Sampling of Archival Records	55
Participant Solicitation and Navigation of Web-based Assessment	55
Usable Sample Prerequisites	57
Statistical Analyses, Planned	58
Summary	58
 IV. Analysis	 59
Overview	59
Interactivity Content Analysis	59
Sampling Results	60
Construct Measurement Formulas	63
Non-CBT Instructional Exposure (NIE) Survey Reliability	66
Statistical Analyses, Actual	66
Learning Effectiveness and Knowledge Retention, Entire Sample Set	67
Hypotheses Testing	70
Hypotheses 1, Overall Interactivity and Learning Effectiveness	70
Time and Knowledge Retention	71
Hypothesis 2, Overall Interactivity and Knowledge Retention	73
H2 and H3: Multiple Variable Effects on Knowledge Retention	78
H4 and H6: Job Field and Exploratory Demographic Effects on Knowledge Retention	83
H5: Job Field and Non-CBT Instructional Exposure	86
Hypotheses Testing Summary	87

	Page
Other Analyses	90
Retraining Intervals for Network End-users, New Test Score Confidence Intervals.....	90
New Percent Score between NUL and USC/WIAT Treatment Groups.....	92
Control and Treatment Groups.....	92
Non-CBT Instructional Exposure (NIE) Descriptive Statistics.....	93
Summary.....	95
V. Discussion and Conclusions	96
Introduction	96
Limitations.....	96
Discussion of Hypotheses Findings.....	97
Learning Effectiveness.....	98
Knowledge Retention.....	99
Job Field, Knowledge Retention and Non-CBT Instructional Exposure	101
Implications for Academia and Future Research	102
Implications and Recommendations for Practitioners.....	103
Conclusion.....	106
Appendix A: AFCA NUL CBT screenshots with narrative	109
Appendix B: WPAFB User Sate CBT (USC).....	116
Appendix C: WIAT Course Exam.....	125
Appendix D: Web-based retest/survey (AF-wide NUL users)	130
Page 1	130
Page 2	132
Page 3	141
Appendix E: Web-based retest/survey (WPAFB USC/WIAT users).....	142
Page 1	142
Page 2	144
Page 3	153
Appendix F. Email Participation Request.....	154
Bibliography	155
Vita.....	161

List of Figures

Figure	Page
1. Interactivity Measurement Matrix.....	21
2. Preliminary Research Model.....	26
3. Synthesized Research Model.....	44
4. Overall Interactivity Content Analysis Methodology.....	48
5. Knowledge Retention Time Series, Relative Retained Knowledge.....	75
6. Hypothesis Testing Results, Synthesized Research Model.....	89
7. Retraining Interval Visualization: New Test Score Confidence Intervals....	91

List of Tables

Table	Page
1. Instructional Domains and Mediums: Training, Awareness, and Education	41
2. Hypotheses.....	43
3. Quasi-experimental Design.....	48
4. Interactivity Content Analysis, Results.....	60
5. Sampling Results.....	61
6. Sample Demographics.....	62
7. Construct Measurement Formulas.....	63
8. Non-CBT Instructional Exposure Recoding Scheme.....	64
9. Non-CBT Instructional Exposure Medium-Specific Weighting.....	65
10. NIE Correspondence Analysis.....	66
11. Learning Effectiveness and Knowledge Retention Among All Sample Groups and Across All Retention Intervals.....	68
12. Raw Knowledge Loss Analysis, (T1 - T2).....	69
13. Hypothesis 1: Effects of Overall Interactivity on Learning Effectiveness, Treatment Group Analysis.....	70
14. Time Effect (Days Passed) on Knowledge Retention (Relative Retained Knowledge) using SLR and single parameter t-tests.....	72
15. Linear Equations for Relative Retained Knowledge by Days Passed.....	73
16. New Test Score, Knowledge Retention, and Knowledge Loss Measures within Month Group Retention Intervals.....	74
17. Days Passed between Overlapping Retention/Month Groups for Treatment Group, Welch ANOVA.....	77

	Page
18. Overall Interactivity effect on Knowledge Retention: Relative Retained Knowledge between Treatment Groups and Retention/Month Groups.....	77
19. Non-CBT Instructional Exposure (NIE) Distribution Characteristics.....	78
20. ANOVA, Days Passed within Independent Variable Sets, Both Treatment Groups, Retention Intervals 2-8 months.....	79
21. MLR on Time, Overall Interactivity, and Non-CBT Instructional Exposure effects on Knowledge Retention (Both Treatment Groups, Retention Intervals 2-8 months).....	80
22. MLR on Time and Overall Interactivity effects on Knowledge Retention (Both Treatment Groups, Retention Intervals 2-8 months).....	80
23. MLR: Non-CBT Instructional Exposure (NIEWA) effects on Knowledge Retention.....	82
24. Knowledge Retention and Time ANOVAs, NUL Treatment and Control Group (n = 360).....	84
25. Knowledge Retention and Time ANOVAs, USC/WIAT Treatment and Control (n = 384).....	85
26. Job Field effect on Non-CBT Instructional Exposure.....	86
27. Hypothesis Testing Results Summary.....	88
28. Retraining Interval Assessment: New Test Score Linear Equations and Mean Confidence Intervals.....	91
29. NUL Users (Treatment and Control): Non-CBT Information Assurance Instructional Exposure Frequency Reporting, Proportion Statistics.....	94
30. USC/WIAT Users (Treatment and Control): Non-CBT Information Assurance Instructional Exposure Frequency Reporting, Proportion Statistics.....	94

List of Equations

Equation	Page
1. Non-CBT Instructional Exposure Weighted Average (NIEWA).....	65
2. Basic Simple Linear Regression Formula for Single Quantitative Parameter	72
3. First Order Linear Model Equation, Knowledge Retention.....	81
4. NUL Treatment Group Response Function, MLR on Time and Overall Interactivity Effects on Knowledge Retention.....	81
5. USC/WIAT Treatment Group Response Function, MLR on Time and Overall Interactivity Effects on Knowledge Retention.....	81

Abstract

The United States Air Force (USAF) currently employs the use of computer-based training (CBT) across a host of requirements. One such requirement is in the Information Assurance (IA) arena and involves the training/licensing of over one-million computer network end-users. USAF use of CBTs has been shown to possess a potential for substantial fiscal savings. However, studies investigating the learning outcomes of learning effectiveness (initial learning) and knowledge retention (sustained learning) associated with USAF CBTs are lacking.

Currently, two USAF CBTs with sizeable user populations are used for the purpose of end-user network training/licensing: the Air Force Communications Agency's Network User Licensing (NUL) CBT and the Wright-Patterson Air Force Base (WPAFB) User SATE CBT / WPAFB Information Assurance Test (USC/WIAT).

Interactivity has been described as one of the most important components of the learning experience (Jung et al., 2002). The primary design difference between the NUL and USC/WIAT CBTs was levels of interactivity – assessed as *Low* (NUL) and *None* (USC/WIAT). Utilizing a quasi-experimental method, this study analyzed the effects of interactivity on learning effectiveness and knowledge retention. Findings include support for a positive relationship between interactivity and knowledge retention. Interactivity was not shown to positively affect learning effectiveness but an exam implementation difference between the two CBTs, namely pass/fail thresholds, is theorized to have significantly increased learning effectiveness. Support for this claim is contained within

goal-setting theories, which purport that when realistic and challenging goals are set, individuals strive to achieve those goals (Latham and Locke, 1984).

The USAF also realizes that IA awareness and training should extend beyond CBTs and directs the implementation of a broad multifaceted strategy. Literature has stated that practice and learning that is related to, and occurs after, initial training can affect knowledge retention (Wisher et al., 2001). In this study, the concept of related practice/learning beyond CBTs is termed non-CBT instructional exposure and was assessed via a survey instrument. The effect of non-CBT instructional exposure on knowledge retention was also explored and evidence for a positive relationship between these two constructs was found.

Other study contributions included significant practitioner-oriented findings. Support was found for fairly robust and diverse IA awareness and training programs both across WPAFB and the Air Force. Knowledge levels of end-users at the currently imposed one year retraining timeline were also assessed. The average of NUL new test scores at the one year point is projected to be $70.4 \pm 4.5\%$, slightly above the 70% pass/fail threshold. The average of USC/WIAT new test scores at the one year point is projected to be $73.9 \pm 4\%$, below the 83% pass/fail threshold.

Recommendations for improving each CBTs design, implementation, and learning outcome results were also made and included: (1) an update/refresh of both CBTs' content and exams, (2) an increase in both CBTs' interactivity levels (3) an increase in pass/fail threshold for the NUL CBT, (4) the implementation of course testing controls for both CBTs, and (5) the use of existing and emerging adaptable learning technology platforms in future CBT versions.

THE EFFECT OF INTERACTIVITY AND INSTRUCTIONAL EXPOSURE ON
LEARNING EFFECTIVENESS AND KNOWLEDGE RETENTION:
A COMPARATIVE STUDY OF TWO U.S. AIR FORCE COMPUTER-BASED
TRAINING (CBT) COURSES FOR NETWORK USER LICENSING

I. Introduction

Background

Government and civilian organizations alike have longed to discover new and innovative ways of creating more effective and efficient employee training programs. Utilizing technology in learning and training environments has been one such way to do so. The earliest roots of technology use in education can be traced to the works of Pressley in the 1920s and Skinner in the 1950s with teaching machines (Dixon-Krauss, 1996). Teaching machines were designed to provide response sensitive feedback to each student thus creating an interactive and individualized learning experience. The concept of interactivity describes the degree to which learning environments facilitate active student participation in the learning process (DeVries and Wheeler, 1996). Although teaching machines had high aspirations, the technology of the past did not possess adequate processing power or software capable of a high level of adaptation (Wiggs and Seidel, 1987). Although teaching machines evolved and improved, the advent of the microcomputer drastically altered technology-based training and teaching machines gave way to computer-based training (CBT). Today's Internet-enabled technology-based training landscape has spawned a highly dynamic online CBT also known as web-based training (WBT).

Due to the proliferation of Internet technologies, online CBTs are currently experiencing tremendous growth. A 1999 CBT study reported that 54 percent of individuals polled said that their companies deliver training or facilitate learning via the World Wide Web (Boisvert, 2000). Some industry experts further predict that WBT will constitute half of all training in the next few years (Roberts, 2001). WBT implementations can greatly expand upon the individualized instructional aim of teaching machines and CBT by utilizing today's tremendous microprocessor capabilities, multimedia applications, and Internet connectivity. Typical CBT products are disseminated through the mailed distribution of CD-ROMs and accessed through a computer's CD drive. WBT differs from CBT in one main way - content location. WBT content is located on a centrally located server. End-users access WBT courses via a web browser, therefore eliminating the need for CD distribution. This also allows WBT to inherit the highly dynamic characteristics of web-site content.

Benefits and Costs of CBT

Organizations typically transfer training materials into computer environments for one of three main reasons: "(1) the desire to customize learning environments to the changing needs of learners, (2) the need to improve how training-related administrative tasks are managed, and (3) the desire to reduce the cost of training" (Boisvert, 2000: 36). This last reason of fiscal savings seems to be the foundational reason why most companies are so attracted to CBT technologies (Perry and Hemstritch, 1986: 33). Whether or not they are classroom or computer-based, training programs cost money to develop. With a significant workforce, larger companies can take greater advantage of economies of scale and more easily overcome CBT developmental and design costs.

These economies of scale are especially appropriate for training programs aimed at a substantial portion of a large organization's workforce with which classroom based instruction would be extremely cost prohibitive. One such large organization with an inclination towards CBT is the U.S. Military.

Military Use of CBT

Historically, because of its large training requirements, the U.S. military has been at the forefront of instructional technology implementation and research (Fletcher and Rockway, 1986). The Department of Defense (DoD) has supported CBT research since the 1960's (Johnston, 1995). The attractiveness of CBT for the military lies in its standardization, scalability, and potential for increased efficiency - both in terms of user-time and training budgets. By transitioning from traditional classroom training to web-based training, some companies have realized up to 75 percent savings in their training budgets (Brown, 2000). Avoided costs include: travel expenses, instructor fees, facility costs, and especially crucial in a military environment - lost time on the job. Orlansky and String (1979) evaluated 30 studies and found that computer-assisted instruction (CAI) courses (previous term for CBT) used in military training were completed in about 30 percent less time when compared with conventional classroom based instruction. Therefore cost savings associated with CBT were based upon estimates of pay and allowances of students for job-time saved. Orlansky and String (1979) also noted that costs attributed to the development, design, and implementation of CAI were not taken into account. However, a *potential* for substantial cost savings through CBT was demonstrated.

Recognizing this potential, the U.S. Air Force (USAF) currently operates a centrally managed AF-wide online CBT program with over one-thousand courses (Mucklow, 2000). This program is known as United States Air Force Computer-Based Training (USAF CBT) system. The USAF CBT webpage is currently located at <http://usaf.smartforce.com>. The USAF CBT program is managed by the Air Force Communications Agency (AFCA) and operates in much of the same ways as typical corporate systems. The USAF CBT program is also known by its company designer namesake and software application name, Smartforce. Training content is available to authorized and registered users either directly via the web or through distributed CDs. This design and operation of USAF CBTs contains aspects of both CBT and WBT but it is typically referred to as CBT. Future references to this AFCA managed AF-wide CBT program will be USAF CBT. The USAF CBT program offers “flexible, adaptable training in the face of spiraling TDY costs and lack of funding for traditional training opportunities” (AFCA, 2002). The vast majority of USAF CBT courses are on information technology (IT) subjects (Mucklow, 2000). The volatile nature of this discipline matches well with the potential for dynamic updates to online CBT courses. Registration and access to CBT courses is open to all AF members; active duty, reservists, government civilians; sister service members; and for Information Assurance (IA) courses, also open to government contractors. Although the Air Force operates a central CBT program, some bases have chosen to develop their own online training courses. One such base is Wright-Patterson Air Force Base (WPAFB), located in Ohio.

Information Assurance Training

Information Assurance is defined in AFI 33-204 as “information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation” (DAF, 2001: 10). With the enactment of Public Law 100-235 (1988), commonly referred to as the Computer Security Act of 1987, the U.S. government recognized the need for training all end-users utilizing government information systems. This act requires all individuals involved in the “management, use, or operation of Federal computer systems” to receive mandatory periodic training”. In that the vast majority of government employees now access Federal computer networks as part of their regular duties, this Information Assurance training directive is an enormously large endeavor. Further expanding the already substantial population, the interpretation of the Computer Security Act has included all individuals, who utilize Federal computer networks, including government contractors, as needing this periodic training.

The U.S. Air Force, falling under the administration of the Federal government, is also required to train its network users. Although just one military service, the Air Force is responsible for a substantial population, consisting of approximately 719,000 total personnel (active-duty, civilian, guardsman, and reservists) as well as an abundance of government contractors (AFPC, 2002). As a technically oriented service, one may assume that the vast majority of the Air Force’s 700,000 plus personnel are network users. When supplemented with government contractors, this training requirement easily exceeds one million end-users. The USAF meets this network user training requirement through its administration of a network user licensing program outlined in Air Force

Instruction (AFI) 33-115v2, Licensing Network Users and Certifying Network Professionals (DAF, 1999). This AFI describes the training requirement and informs units of the existence of a centrally managed computer-based training course at the USAF CBT central site that can be used to meet this requirement. Licensing can be accomplished through the completion of a particular USAF CBT course or through locally developed training programs. Annual refresher training of individuals already licensed or recently relocated is an additional requirement of licensure. The refresher training requirement can be accomplished through the re-completion of a USAF CBT or local course.

Information Assurance Training in a CBT Domain and Beyond

As mentioned, there are CBTs both AF-wide and base-specific. This is the case for network user training. There are two CBT courses used for licensing network users that affect large populations. One CBT course is managed under the auspice of the USAF CBT and one is managed by the 88th Communications Group (88 CG) at Wright-Patterson AFB. Both courses are of one hour duration. The USAF CBT used for training computer network end-users is titled Network User Licensing (NUL). Although its use is not mandated, NUL is used AF-wide and has the potential to reach well over one million users. It has become the de facto training standard for satisfying the requirement specified in AFI 33-115v2. The CBT at WPAFB used for training computer network end-users is titled the User SATE (Security, Awareness, Training, and Education) CBT (USC) with the test portion of the course titled the Wright Patterson Air Force Base Information Assurance Test (WIAT). The WPAFB CBT will be referred to herein as the

USC/WIAT. The USC/WIAT is accessible to over 60 diverse AF and DoD organizations comprised of over 22,000 government personnel and contractors (ASC PA, 2002).

It is evident from the estimated number of users that both NUL and USC/WIAT attempt to reach, one million and twenty-two thousand respectively, that the use of classroom-based training for network user licensing is not economically or logistically feasible. CBT technologies meet the need for licensing network users by simplifying program management, standardizing content, and providing cost savings potential. It is evident that CBT will remain the instructional medium of choice for licensing network users. However, this realistic outlook of CBT as the principal training means for IA training should not cause a sense of complacency in assuming that current implementations are achieving acceptable levels of learning outcomes.

For issues as important as Information Assurance training, the Air Force recognizes the need to utilize communication mediums outside of CBT in order to reinforce and supplement learned knowledge. AFI 33-204, titled Information Assurance Awareness Program, directs unit IA awareness and training managers, referred to as workgroup managers, to implement broad IA awareness outreach plans that utilize several delivery mediums such as: posters, flyers, videos, public service announcements, newspaper articles, screen savers, and base television channels (DAF, 2001: 6). Workgroup managers, although responsible for disseminating IA material to their unit's personnel, do not need to necessarily develop such material. The development responsibility resides further up the chain of command, with AFCA and Major Command (MAJCOM) IA offices.

Problem Statement - Research Questions

Previous studies of military CBT have focused on cost-effectiveness (Orlansky and String, 1979), or planning, selection, and implementation issues (Nason, 1992). The primary research question in this study is to assess the learning outcomes (learning effectiveness and knowledge retention) associated with the NUL and USC/WIAT CBTs. Research has demonstrated that the interactivity levels of technology-based instructional courses can have a significant effect on learning effectiveness and knowledge retention. However, there is a lack of evaluative studies on military CBTs that focus on the effect of interactivity on learning effectiveness and knowledge retention. The main objective of any training program is to instruct employees in some type of subject matter, increase their knowledge and understanding of that subject, and ultimately affect their future behavior in encountering situations applicable to that training. In the realm of network user training, these objectives apply. End-users must learn the nature of the government computer network domain, assess current threats and vulnerabilities, and learn what measures they can take to mitigate risk of system compromise.

There are certain characteristics inherent to CBT and WBT programs. Organizations do not have to abide by set standards when designing and implementing CBTs or WBTs. For this reason, there is a multitude of different styles and designs of CBTs. CBTs exist which incorporate varying levels student interactivity in their design. This research study has the unique opportunity to test the effect of CBT interactivity in a military training environment on learning effectiveness and knowledge retention.

Many experienced IA professionals have stated that obtaining a strong IA posture depends on individuals more than on technology (Desman, 2002; Kabay, 1994; Siponen,

2000). A Chairman of the Joint Chiefs of Staff Instruction on defensive information operations recognizes that “the *employee* is the essential element of a successful protection program” (DoD, 1997: App H). Air Force Policy Document 10-20 (DAF, 1998: 4) also notes that “successful defensive counterinformation operations begin with each *individual* accepting and carrying out his/her responsibilities in protecting information and information systems from attack and exploitation.”

End-user training affects the overall security posture of enterprise information and network systems. In order to assess whether or not network users are being effectively trained through the use of CBT courses, detailed studies on learning outcomes must be performed. The Federal Information Security Assessment Framework (FISAF), published by government Chief Information Officers (CIOs), recognizes the need for such assessments as evidenced by its declaration of the need to not only train employees on security requirements but to “plan, implement, maintain, and evaluate an effective training and awareness program” (FISAF, 2000). This study sets out to accomplish an evaluation of training. Perry and Hemstritch (1986) note that CBT is one medium by which learning can take place; as with all other mediums the assessment of student learning is an essential task of teaching. Without a valid assessment of end-user information assurance training competency, the protection of our military networks, the security of our nation, and lives of our people are at risk. How can the USAF fortify its information security posture if uninformed decisions based upon unfounded claims regarding the state of network security are made?

It is not clear to what level local IA managers utilize non-CBT material for accomplishing IA training and awareness objectives. An additional research question

asks: how robust and diverse are USAF IA training and awareness programs? An assessment of IA training and awareness programs AF-wide could prove beneficial in identifying a current baseline of program characteristics.

Scope

This study's scope focuses on four primary constructs: interactivity, learning effectiveness, knowledge retention, and non-CBT instructional exposure. In that these constructs are discussed within this chapter, the following definition of terms is appropriate. Background and further discussion of each construct will be covered in Chapter II.

Interactivity describes the degree to which a learning environment facilitates active student participation in the learning process (DeVries and Wheeler, 1996). Learning effectiveness describes an initial amount of learning which occurs directly following some form of instruction (Fletcher, 1996; Johnston, 1995; Kulik and Kulik, 1991; Niemiec and Walberg, 1987). Knowledge retention describes a sustained level of learning over time and relative to initial learning (Hulse, et al., 1980). Instructional exposure describes a level student contact with material relevant to initial learning content. This study focuses upon instructional exposure outside of the original teaching medium of CBT and terms this construct as non-CBT instructional exposure.

This study is measuring the learning outcomes of two far-reaching computer-based training courses in the subject area of computer use and network security. Both of these courses are used by the USAF in licensing its members for access to its computer networks. Both courses have extremely similar course content and contain near identical end-of-course exams. The NUL CBT is used across the entire Air Force by active duty,

guard, reserve, government civilians, government contractors, foreign/local nationals, and USAF Academy cadets. Total potential users for the NUL are in excess of one million individuals. The USC/WIAT serves an identical user demographic less USAF Academy cadets and can potentially reach users in excess of twenty thousand individuals. This study aims to analyze the learning outcomes (learning effectiveness and knowledge retention) demonstrated by each CBT user group.

As previously mentioned, AF instructions advocate for IA training and awareness that incorporate mediums beyond CBT. This study is also aimed at assessing the robustness and diversity of information and network security training and awareness programs beyond CBTs and AF-wide. The effect of this non-CBT instructional exposure on the learning outcome of knowledge retention is also evaluated.

Contribution to Researchers and Practitioners

This study's primary contribution to research is to determine the effects of varying levels of military CBT interactivity and non-CBT instructional exposure on learning effectiveness and knowledge retention. The author has the unique opportunity to assess similar course contents implemented in two different interactive CBT designs across substantial populations. The findings of this study may serve as a foundational work that establishes the effects of varying CBT design characteristics and provides a model from which to assess CBT learning outcomes. This study may also serve as a baseline measurement for the effectiveness of the CBTs of interest.

This study also has important practical implications. Currently, policymakers are reassessing the need for annual network security refresher training. This study hopes to outline the time interval at which users drop below an acceptable level of knowledge and

consequently provide military leadership with statistics upon which to make informed decisions on imposing a standard retraining interval.

The AF instructs workgroup managers to make use of training mediums beyond CBT (DAF, 2001). There are myriad communication mediums available to unit workgroup managers which they can use to reinforce and expand upon concepts in the CBTs. The usage level of various training and awareness mediums by workgroup managers is currently unmeasured. This study will attempt to assess the robustness and diversity of IA-specific training and awareness exposure beyond CBT. The overall term that will be used for describing an individual's contact with IA material beyond CBT is non-CBT instructional exposure (NIE). In doing so, this research may identify key strengths and weakness trends across the AF. AF leaders may then focus energies in improving identified weaknesses. This can lead to the strengthening of the overall information security and assurance posture force-wide. This study may also serve as a baseline measure of communication medium use on which to base future assessments.

Summary

This chapter has provided a background on computer and web-based training and addressed its uses in a military environment. Specifically covered was the USAF's use of CBT for satisfying the computer network user training requirement mandated by the Computer Security Act of 1987 and outlined in AFI 33-115v2. This chapter briefly reviewed two CBT implementations for licensing network users. Covered was the lack of formal evaluation of military CBTs in terms learning outcomes. Discussed was the need to assess the robustness and diversity of USAF IA training and awareness programs beyond CBT. The scope of this research is limited to the AF population and particular to

the concepts of interactivity, learning effectiveness, knowledge retention, and non-CBT instructional exposure.

Chapter II will review literature on learning theories and teaching strategies related to computer-based training and interactivity as well as studies on learning effectiveness and knowledge retention. The next chapter will also provide a more detailed background into the history and nature of the CBT courses being evaluated (NUL and USC/WIAT). Primary hypotheses will be proposed in reference to the effect of interactivity on learning effectiveness and knowledge retention, as well as the effect of non-CBT instructional exposure on knowledge retention. Chapter III will outline the methodology used in testing the proposed hypotheses. Chapter IV will detail the results of analyzing archived and newly collected data. Finally, chapter V will discuss the results of the analyses as well as academic and practitioner implications and recommendations.

The electronic .pdf version of this document contains clickable hyperlinks within the table of contents, list of figures, tables, and equations as well as Adobe bookmarks which link to applicable document sections.

II. Literature Review

Overview

This chapter provides a review of relevant literature on learning theories and teaching strategies most relevant to interactivity in a computer mediated environment such as CBT. The two CBTs of interest, the USAF NUL CBT and WPAFB USC/WIAT CBT, will be referred to herein as simply NUL and USC/WIAT. Also covered will be literature and studies dealing with CBT learning effectiveness and knowledge retention.

In order to familiarize the reader with the nature of CBTs, this chapter provides an overview of such programs and also covers the specific implementation characteristics of the NUL and USC/WIAT CBTs. Realizing that instructional efforts extend beyond CBTs, a review of the domains and mediums by which Information Assurance content is conveyed to employees is reviewed. These domains and mediums are reviewed in order to provide a framework for the construct of non-CBT instructional exposure. This chapter will conclude with the presentation of several hypotheses. The hypotheses set forth will be based upon the reviewed literature and content analysis differences identified between NUL and USC/WIAT.

Learning Theories and Teaching Strategies

There is a multitude of learning theories and teaching strategies in the educational domain. Learning theories attempt to explain the process and nature by which individuals process and acquire knowledge. Explaining such a complex and intangible process as learning is not an easy endeavor. There are major disagreements in the fields of teaching and learning as to how students come to internalize knowledge. Teaching

strategies attempt to provide methods for educators to enhance and improve the knowledge acquisition process. In the design and implementation of various CBT courses, one observes some commonalities within the theoretical, strategic, and procedural foundations of teaching and learning. A qualitative review of both the NUL and USC/WIAT CBTs has resulted in the emergence of a limited set of applicable theories and strategies. Those emerging theories and strategies will now be discussed in detail.

Learning Theories and CBT

With a preliminary review of both the NUL and USC/WIAT CBTs, the author observed the emergence of two main theoretical frameworks; constructivist and sociocultural. As noted, there is a substantial academic debate about the nature and psychology of learning. Many researchers and theorists have suggested that the constructivist and sociocultural perspective are congruent while many others contend they are opposed in some of their basic underlying assumptions about the way in which things come to be and in the nature of truth (Packer and Goicoechea, 2000). Important to note is White's (1993: 620) acknowledgment that "there is no one theory about the psychology of pedagogy that we can identify and teach with confidence that others are wrong." The purpose of this research is not to debate the merits of the congruence or opposition between the constructivist and sociocultural learning theories. The debate itself suggests the existence of some evidence for both sides of the argument. In the context of computer-based training, both theories seem to have applicability and merit. Therefore, the author chooses to assume at least a partial congruence between these two theories and proceed.

Sociocultural Theory of Learning

The sociocultural theory of learning was pioneered by Lev Vygotsky in the early twentieth century Soviet Union. Although his works were not published outside the Soviet Union until the 1960s, his sociocultural theory currently resides as one of the main theories of learning used in Western thought today (Dixon-Krauss, 1996). Vygotsky's theory of social development states that social interaction is fundamental to learning (Moll, 1990; Rogoff, 1990; Packer and Goicoechea, 2000; Vygotsky, 1986). The term *scaffolding* is used to represent a guiding of student by teacher, whereas the teacher or *knowledgeable other* draws a learner from their achieved level of performance on a gradual path to their potential level of performance. The range between the two levels of performance is known as the *zone of proximal development (ZPD)* (Bigge and Shermis, 1999; Dixon-Krauss, 1996; Moll, 1990; Rogoff, 1990; Vygotsky, 1978; Vygotsky, 1986). This interaction between student and teacher is the social component that Vygotsky would contend is crucial to learning and that makes cognition a complex social phenomenon (Dixon-Kraus, 1996).

Vygotsky also believed in the social use of sign systems as mediators between learners and their potential level of development (Moll, 1990; Rogoff, 1990; Vygotsky, 1978; Vygotsky, 1986). Vygotsky's sign systems include communication mediums such as language, writing, and number systems; and sign systems can be extended to the computer-aided multimedia environment of CBTs (Dixon-Krauss, 1996; Vygotsky, 1978: 7; Vygotsky, 1986). The process of scaffolding requires the presence of Vygotsky's knowledgeable other. In the case of CBT, the social interaction may be interpreted as occurring between the individual and the computer, with the computer acting as the

“knowledgeable other” (Bigge and Shermis, 1999; Dixon-Krauss, 1996; Moll, 1990; Rogoff, 1990). This social scaffolding process may work best when a high level of interactivity within a CBT exists. The interactivity level of CBT courses is dependent mainly upon the design of the courseware. The potential exists for CBT programs that are highly interactive, mimicking the social interaction of student-teacher whereas computers guide students towards their potential level of performance. Those CBTs with a high level of interactivity in their course design can be viewed as implementations incorporating a sociocultural framework into the teaching method.

Constructivist Theory of Learning

Constructivist theory contends that learning is an active process in which students construct new ideas or concepts based upon their current and past knowledge (Dixon-Krauss, 1996; Fox, 2001). This theory also contends that meaning is constructed through interactions with one’s environment either individually or with others (Packer and Goicoechea, 2000; Wonacott, 2000). The instructor is considered to be a facilitator whose main purpose is to engage the learner (Wonacott, 2000).

CBTs allow individuals to dynamically construct meaning by interacting within a computer-mediated environment and appending that meaning to preexisting knowledge in a particular subject area. However, an individual’s ability to self-learn is limited by the baseline level of knowledge extant before engaging in the training. Often, this knowledge is somewhat limited. In such a case, the use of a sociocultural scaffolding technique would be appropriate in order to more closely guide an individual along a path of knowledge construction.

Sociocultural and Constructivist Learning Theories

Some congruence between a sociocultural learning theory and constructivist approach can be shown in their dependence upon some type of mediation between a learner and their acquisition of knowledge. The constructivist perspective describes learning as an active process and also stresses the importance of engaging the learner. This engagement of the learner is facilitated by an entity outside the learner; most times a live teacher. This engagement often requires a social interaction between a learner and a knowledgeable other. Both theories describe the process of learning as moving learners from their current state of knowledge and understanding to a higher level; the term knowledge construction is used in a constructivist interpretation while scaffolding is used in a sociocultural approach. This leads to a discussion of the implications of both theories (constructivism and sociocultural) on applicable teaching strategies present in CBTs.

Teaching Strategies and CBT

Teaching strategies refer to methods that educators implement in order to facilitate and improve learning. In this sense, the combined strategies that an educator uses can collectively reflect an underlying pedagogy. An effective CBT reflects such pedagogical dimensions throughout its design and operation. For the purpose of this research, three strategies will be reviewed: individualized instruction, interactivity, and programmed instruction.

Individualized Instruction

Individualized instruction focuses on the “efficient delivery of knowledge and skills based upon the learner’s characteristics and needs” (Kerka, 1986: 1). CBTs have the potential to be effective for a variety of learners. This is especially beneficial for training programs aimed at a mass amount of employees, like the USAF network user licensing program. This broad learner effectiveness is rooted within CBT’s ability, but not always its implementation. These strategies can provide multiple pathways of instruction for different learners. Furthering the ability to individualize instruction, CBTs can accommodate multiple intelligences and learning styles through software design (Wonacutt, 2000).

CBTs can be designed to adapt to an individual’s learning preferences. Designs can allow users to travel along the training content in a nonlinear pattern specific to their own choices. However, the level of learning individualization rests upon the design and implementation of CBT course content. Three design implementations and teaching strategies that can enhance individualized instruction are the use of interactivity, multimedia, and programmed instruction

Interactivity

The concept of interactivity describes the degree to which learning environments facilitate active student participation in the learning process (DeVries and Wheeler, 1996). Independent of teaching mediums (conventional or computer-based), interaction is accepted as one of the most important components of the learning experience (Jung et al., 2002: 153; Muirhead, 2000; Oliver et al., 1996; Vygotsky, 1978). To clarify, interactivity describes a characteristic of a learning environment, while interaction is a

process which describes the desired outcome of an interactive environment, which is communication between two or more entities (Sutton, 2001). Historically, interaction has been primarily understood in a face-to-face communicative learning context (Kettanurak et al., 2001). However, computers now possess an increased capability to imitate human-to-human interactivity in a human-to-computer context. In a computer-mediated environment, interactivity exists along a continuum and can be defined as the “degree to which technology supports/enables interaction resembling human conversation” (Kettanurak et al., 2001: 545). Computer technology has the ability to provide individualized instruction by designing interactive learning environments (Perry and Hemstritch, 1986). Highly interactive learning environments are described as: where the learner is able to receive all necessary clarifications, immediate feedback, and personal attention (Kerka, 1986; Kettanurak et al., 2001).

There are many different types of interaction that have been documented and described in current literature. However, this research endeavor is focused solely upon interaction between one student and a computer. This student-computer interaction, also referred to as learner-online resource or learner-content interaction, is encompassed within the definition of academic interaction from Jung et al. (2002) and Paulsen’s (1995) definition of one-alone computer mediated communication (specific to online applications).

The nature of interactivity suggests foundations in both constructivist and sociocultural learning theories. Interactivity’s aim is to imitate a social encounter between two human beings (sociocultural) in order to facilitate learning. It has also been

proposed that an instructional system possessing greater interactivity “will more actively engage the learner” (constructivist) (Kettanurak et al., 2001: 545).

In a CBT environment, interactivity levels can be measured in three main ways; frequency, range, and modality (Kettanurak et al., 2001). Kettanurak et al. (2001: 545) defines these aspects of interactivity as follows: (1) *frequency* is a measure of how often user input is enabled, (2) *range* describes the range of choices available to a user at a given moment (binary (yes/no) would be considered a narrow range), (3) *modality* as the use of either single or multimedia delivery medium features. Modality, as a third aspect of interactivity, will be covered individually and in greater detail in the next section on human perception. Figure 1, excerpted from Kettanurak et al. (2001: 550), portrays a matrix method with 18 distinct cubes by which to rate a CBT’s level of interactivity. The lowest level of interactivity is represented by the cube labeled *Low*, which indicates a single media, low frequency, and low range. The highest level of interactivity is represented by the cube labeled *High*, which indicates the use of multiple media accompanied with high frequency and high range.

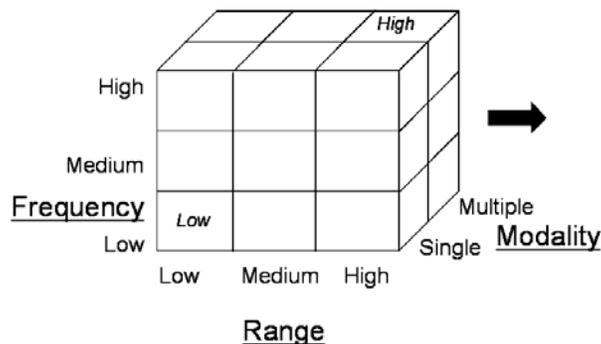


Figure 1. Interactivity Measurement Matrix (Kettanurak et al., 2001: 550)

Kettanurak et al. (2001) also propose learner control as a key component of interactivity. Learner control in a CBT environment can be manifested through a learner's ability to control the pace and order of instruction, often observable through one's power to navigate through course content.

Studies on the effect of interactivity on learning effectiveness (student performance) in a military CBT environment are lacking. The Kettanurak et al. (2001) study analyzed only the effects of the control component of interactivity on student performance, and found that increased learner control had a negative relationship with performance improvement. This peculiar research finding was believed to be a result of giving learners too much control, by which they were able to skip entire content sections and proceed to course evaluations. Fletcher (1996) reports on six meta-analytic studies of the effect of interactivity on student performance in an Interactive Videodisc Instruction (IVI) environment; all six studies suggest increased interactivity results in increased student performance. Although Fletcher's study (1996) did not report on interactivity in a CBT environment, IVI is a technology-based training environment, and one might extend these findings into a CBT domain.

Human Perception

As noted in the previous section, a modality (delivery medium) can be considered a component of a learning system's interactivity. When delivery mediums are discussed, it is appropriate to address the issue of human perception. Human perception can be defined as the process by which individuals recognize and interpret sensory stimuli in his/her environment (Russell, 2000: 4). Generally, media are defined as a "set of different technologies and contents, often controlled by a computer" (Clark, 1992). In

the context of CBTs, typical media content includes one or more of the following: text, graphics, sound, animations, and video.

The use of multimedia in CBTs can draw upon theoretical aspects from both a constructivist and sociocultural framework. Constructivists might contend that the primary purpose of multimedia would be to engage the learner in the active process of knowledge construction, while socioculturalists might focus upon multimedia's ability to enhance the social interaction between human and computer. Vygotsky (1978: 31) noted as a general law "the dependence of all natural forms of perception on the structure of the sensory field." Multimedia can be viewed as a combination of Vygotsky's sign systems; it can combine the sign systems of text, graphics, sound, animations, and video into coherent and meaningful content. Creating an entertainment-like learning atmosphere may enhance the engagement of learners as well as facilitate a more dynamic social interaction. But what effect might multimedia have on learning effectiveness?

Research studies have found mixed results for the effect of multimedia on learning. Clark (1992) cites studies that found positive support, negative support, and no significant difference for increased learning with multimedia. Michas and Berry (2000) demonstrated significant gains in learning effectiveness with the use of both text and line drawings (simple graphics) over a text-only content presentation. Michas and Berry (2000) also cite support for their finding in previous research studies. The Michas and Berry (2000) study is most applicable for this research, in that the two CBTs differed with one presenting text-only (like USC/WIAT) while the other presented learners with text in combination with simple graphics (like NUL).

Programmed Instruction

Programmed instruction is a progressively monitored, step-by-step discrete teaching method; it conveys small units of learning material at one time, whereby students show competence in one stage before moving on to another (Kerka, 1986: 1). The use of a programmed instructional delivery method is present within many CBT courses (Fletcher and Rockway, 1986). This type of instruction is manifested through the presentation of small manageable units of information, each followed by a short section evaluation section, and then ultimately an end-of-course test that determines an individual's overall competence. Advantages to using programmed instruction can include: an improved organization of knowledge, increased opportunity for interactivity, and immediate performance feedback on competence and progress (Kerka, 1986).

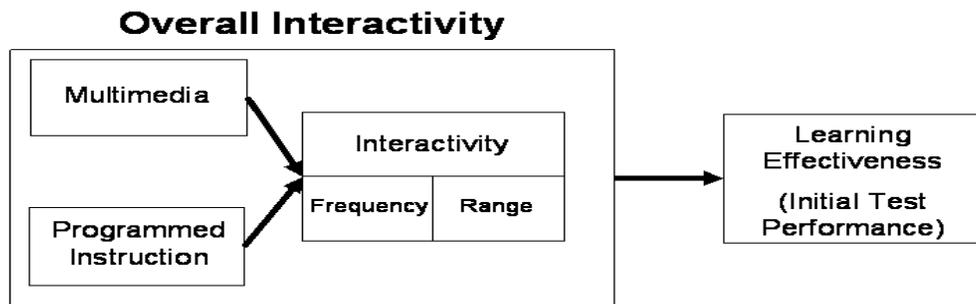
Similar to individualized instruction, interactivity, and human perception; programmed instruction has implications in both a constructivist and sociocultural framework. Programmed instruction supports constructivism in that short manageable sections with assessments can help engage learners and provide them the opportunity to actively take part in the knowledge construction process. This is in comparison to a passive learner taking part in a simple "page-turning" course. The sociocultural aspect of programmed instruction is evident with the increased opportunity for human-computer interaction in a social context to take place.

This author proposes an expansion of the interactivity model from Kettanurak et al. (2001), of which contains a component of programmed instruction in addition to the already present modality, frequency, and range components. Programmed instruction section assessments within a CBT provide the opportunity for learners to interact with the

course material. Learners can demonstrate a mastery of knowledge content or lack thereof. CBT software can respond to individual answers by either providing validation of a correct answer or clarification of a wrong answer by providing justification and possible review of concepts particular to that question. In that interactivity has been shown to have a relationship with student performance, this author proposes that the use of programmed instruction may have an effect on student performance as mediated through a construct of overall interactivity.

Learning Theories and Teaching Strategies Summary

Individualized instruction has been shown to be a desirable design goal of CBTs. Interactivity, multimedia, and programmed instruction have been shown to contribute to the individualized nature of instruction. These strategies have been shown to be grounded in the theories of constructivism and sociocultural learning. CBTs have the ability to individualize the learning process through varying levels of interactivity. However, this ability is dependent upon a course's interactive design characteristics. Interactivity was presented as a measure of the frequency and range of user inputs, multimedia use, and the inclusion/exclusion of a programmed instruction delivery technique. Research has demonstrated a relationship between level of interactivity and learning effectiveness as measured by student performance (Fletcher, 1996). A preliminary research model is presented in Figure 2. Figure 2 presents the graphical use of the term *overall interactivity* which is used in this study to encompass the components of frequency, range, multimedia, and programmed instruction.



**Figure 2. Preliminary Research Model
(Adapted and Expanded from Kettanurak et al. (2001))**

Learning Effectiveness and CBT

The overwhelming majority of studies on the effectiveness of CBT involve a comparison between computer-based training and traditional instructor-led classroom training. The learning effectiveness of a training program is described as the initial learning that takes place as a result of instruction (Fletcher, 1996; Johnston, 1995; Kulik and Kulik, 1991; Niemiec and Walberg, 1987). Learning effectiveness has consistently been measured by student performance/achievement assessed by some type of overall course test. Studies have been conducted in a variety of settings. Of relevance to this research is the effectiveness of CBTs in an adult or military learning environment. Some studies have found a significant difference between CBT and classroom student performance while others have not. A synthesis of these studies is covered through the

review of meta-analytic studies, which by design include research findings of both significant and nonsignificant differences.

Johnston (1995) conducted a meta-analysis of thirty-three empirical studies that compared CBT with conventional instruction in a military training environment. For military training, Johnston (1995) found on average an effect size of 0.27 (controlling for outliers), which can be understood as an overall increase in student achievement for CBT from a 50th to 60th percentile performance. In this same research effort, Johnston (1995) had intended to measure the effect sizes of knowledge retention but was unable to because of a lack of data across the thirty-three investigated studies. In an updated meta-analytic research effort of CBT effectiveness in military training, Fletcher (1996) report an effect size of 0.40, understood as an increase in student achievement for CBT from a 50th to 66th percentile performance.

Other meta-analyses of computer-based instruction (CBI) have found similar student performance effects. CBI is a broad term used that consists of a family of technology-assisted learning methods including: computer-assisted instruction (CAI), computer-managed instruction (CMI), and computer-enriched instruction (CEI). Such studies have found effect sizes ranging from 0.26 to 0.47, translating to student performance improvements ranging from 50th to 60th percentile to 50th to 68th percentile (Fletcher, 1996; Kulik and Kulik, 1991; Niemiec and Walberg, 1987). Although the use of the computer in these environments is not identical to computer-based training (CBT) of today, the use of the computer as a learning medium is a common thread that binds these teaching methods together. One could propose similar student performance effect sizes for CBT.

Knowledge Retention

Psychological literature defines knowledge retention as the ability for an individual to recall or remember knowledge that has previously been learned (Hulse, et al., 1980). Academic studies have measured knowledge retention as some level of knowledge demonstration at some time interval following some type of instruction or training (Haynie, 1997; Rodriguez, et al., 2002; Sanders et al., 2002; Williams and Zahed, 1996; Wisner et al., 2001; Yildrem et al., 2001). In this respect, knowledge retention describes a sustained level of knowledge over time and relative to initial learning (learning effectiveness). The close interrelationship between learning and retention is evident; and as such the relationship between the constructs of learning effectiveness and knowledge retention constructs also are apparent. Important to note is the complementary nature between the construct of knowledge retention and knowledge loss. Hulse et al. (1980: 300) note that “the amount you have forgotten about something equals the amount you originally learned less the amount you have retained.”

It is important to note the potential knowledge retention implications resulting from practice/learning that is both related to and occurs after initial training (Wisner et al., 2001). This concept of practice/learning related to initial training is referred to in this study as instructional exposure. Some experts agree that an assessment of performance some time interval following training (knowledge retention), rather than measures of performance directly following training (learning effectiveness), provide the best assessment of learning outcomes (Sanders et al., 2002). Knowledge retention specific to this research effort refers to the recall of facts, terminology, and concepts at varying time intervals following completion of an initial CBT training course and test.

Scores of literature have demonstrated the time-dependent nature of knowledge retention, whereby as time passes from an initial demonstration of particular knowledge, the ability to recall that same knowledge gradually declines, regardless of delivery medium (Hulse et al., 1980). Psychological research in this area has demonstrated that “forgetting newly acquired knowledge occurs naturally over periods as short as several hours to as long as many years” (Wisher et al., 2001: 20). Although particular types of knowledge exhibit different rates of decline, the general behavior of knowledge retention curves exhibit: a rapid decline shortly after initial training, followed by a continuous slight decline, and finally an asymptotic leveling (Hulse et al., 1980). Several studies have demonstrated that a majority of knowledge loss tends to occur within the first ten weeks after initial training (Wisher, et al., 2001).

Kulik and Kulik’s 1991 meta-analysis demonstrates that knowledge retention in academic studies has consistently been measured by the amount of course content (either raw correct or percentage correct on an end-of-course exam) recalled by students who previously took part in a training course at a given point in time. As noted, a knowledge retention calculation needs to be formulated relative to initial knowledge demonstration. Therefore, knowledge retention can be measured as *relative retained* knowledge and calculated as: the performance on a retention exam in relative to performance on an initial exam $[(T2/T1) \cdot 100]$. The complement of knowledge retention can be described as *relative knowledge loss* and calculated as: the difference between initial performance and retention performance relative to initial performance $[(T1 - T2) / (T1)] \cdot 100$.

As mentioned, the majority of studies on CBTs involve a comparison against traditional classroom instruction. This is also the case in terms of studies on knowledge

retention in CBTs. Kulik and Kulik's (1991) meta-analysis included twenty studies that examined knowledge retention differences, as measured by percentage correct on follow-up examinations between CBI and traditional classroom instruction. The average retention effect size in the twenty studies was 0.17 (Kulik and Kulik, 1991). This translates to an improvement for knowledge retention from a 50th to approximately a 57th percentile. More recent research by Williams and Zahed (1996) involved just one evaluation, but the study was between CBT and traditional classroom instruction. This study measured student performance directly following coursework and one month after using an identical multiple-choice 33-item exam. Differences between treatments in initial posttest performance directly following coursework were found to be nonsignificant (Traditional: 91.96 mean, 5.23 standard deviation (SD); CBT: 89.78 mean, 7.86 SD); However, there was significant CBT advantage on the retention test (percentage score) given one month later (Traditional: 78.74 mean, 9.10 SD; CBT: 85.30 mean, 8.01 SD) (Williams and Zahed, 1996)

Thus, there exists at least some evidence that the use of CBT can affect knowledge retention. This author proposes that among CBTs, varying levels of interactivity will have a significant effect on knowledge retention, as measured by relative retained knowledge.

Overview of an Online CBT Program

Many organizations implement comprehensive online CBT programs that offer several courses across different knowledge and skill content areas. Typically, CBTs are centrally managed by software known as a Learning Management System (LMS) (Roberts, 2001). LMSs can involve software and databases associated with course

content and presentation, user registration, and metrics collection/analysis. Such a system usually requires users to first register with the system. This can be accomplished online or through other administrative means. Following registration, users log onto a training website and access the latest course material real-time or choose to download it for later access. If a user chooses to download the course content and train off-line, an eventual reconnection to the central server is needed for recording and tracking of user progress and scoring. The liveplay option reveals the web-nature of online CBTs and involves users directly accessing with course content via an Internet connection by downloading training web-pages “on the fly.” Normally, both liveplay and download modes allow users to perform training over an interrupted period of time; they do not necessitate the completion of an entire course at one session. CBT’s central control of training content allows organizations to provide the most current training to anyone, anywhere, anytime. Online CBTs achieve hardware platform independence beyond that of regular CBTs by normally requiring only a web-browser and possibly some software add-ins/plugin-ins in order to participate in courses.

AFCA NUL CBT (Rogers, 2002)

The NUL is managed by the Air Force Communications Agency (AFCA) and corresponds with course code YAF06SE. NUL was initially one section of a larger CBT, Information System User (ISU), course code YAF01SE. The ISU CBT was a six-hour course and for a short time was required to be completed by all AF network users. However, due to tremendous negative feedback from units on the excessive time requirement of this CBT, AFCA recommended users take only the network security portion of the training in order to fulfill the network user training mandate. The network

security portion of ISU contained both course content and an end-of-section test.

However, the user tracking and management system only recorded test scores for end-of-course tests, not end-of-section tests. It therefore became difficult for unit managers and AFCA to track training data.

The management solution was to separate the network security portion of ISU into its own standalone CBT course. This standalone CBT course was named Network User Licensing, course code YAF06SE. It was initially put online in February of 2002 to test functionality. At this time, a limited number of AF organizations had access to the course. Following a proof of functionality, AFCA publicized the existence of NUL to the AF at large in July 2002. In the period from February to November 2002, over fifty-six thousand individuals have enrolled in the course. Authorized and registered users who need to take the NUL course first logon to the USAF CBT website at <http://usaf.smartforce.com>. Students can, but are not forced to, review the course before taking the online course exam. This is beneficial for users and the Air Force in that users already competent in network security issues can self-exempt from the course, allowing a focus on primary duties (Perry and Hemstritch, 1986).

NUL is similar to traditional online CBTs previously discussed. Users have the ability to use a liveplay or download mode of the course. Also available to units is a CD-based version of the course. Per AFCA, the CD-based version is used by a substantial user population on standalone non-networked PCs due to units strictly abiding by regulations of not letting users on the network until they pass the NUL course. AFCA is responsible for NUL system content and maintains user registration for all USAF CBT

users as well course metrics on student achievement. CBT screenshots from both the NUL course and course exam are located in Appendix A.

WPAFB USC/WIAT CBT

At Wright-Patterson Air Force Base (WPAFB), the 88th Communications Group (88 CG) has the primary responsibility of licensing network users. The 88 CG is part of the 88th Air Base Wing (88 ABW). The 88 CG has developed its own CBT course for the purpose of licensing WPAFB network users, the USC/WIAT. The USC/WIAT course is hosted on a local WPAFB website at <https://www.asc.wpafb.af.mil/base/c4/iaap/usertraining.htm>. This website contains links to a course text at <https://www.asc.wpafb.af.mil/base/c4/iaap/train/train-docs/usertext.doc> (Appendix B) and a course test called the WPAFB Information Assurance Test (WIAT) at <https://www.asc.wpafb.af.mil/base/c4/iaap/train/test.html> (Appendix C). As with NUL, students can, but do not have to, review the course text prior to taking the test. The course text is an online Microsoft Word document with a text only review of IA network security knowledge and skills. The USC/WIAT CBT is much less complex in its design than NUL. USC/WIAT students can choose to view the course text directly from the website or download the course text and either print a paper-based hardcopy or retrieve it electronically at a later time. There is no user registration system for USC/WIAT but user and test metrics for the WIAT test portion are stored and tracked in a database. When users complete the online test, the database captures self-reported demographics as well as the date and score of the test. The database maintains separate records for each individual user, but at most users are present in two records - one initial test record and one refresher. When a user retakes the refresher test, regardless of time-lapse, his/her old

refresher test record is overwritten. This overwriting may have implications for the system's ability to measure actual learning effectiveness via test scores.

NUL and USC/WIAT Objectives and Exams

The purpose of both the NUL and USC/WIAT CBTs is to train network users. This is in order to comply with AFI 33-115v2, Licensing Network Users and Certifying Network Professionals, dated 1 November 1999, which originates from the Computer Security Act of 1987. Each CBTs objectives and end-of-course exams are nearly identical. Both courses contain three primary course sections consisting of (1) *Authorized and Unauthorized Activities*, (2) *Virus Detection and Protection*, and (3) *Backup Strategy* (Appendices A and B). The USC/WIAT course contains an additional section on *Computer Security Controls* containing material on *User Responsibilities* and *Password Policies* (Appendix B). Both courses contain a comprehensive end-of-course exam comprised of twenty-three multiple-choice questions, with one correct answer and three distracters. Twenty-two of the twenty-three questions on each exam are identical in all respects (question wording, answer wording, answer order). The tests differ on question 8, in terms of the question, the answer options, and the right answer. A primary exam difference is the pass/fail thresholds; NUL users must obtain at least 16 out of 23 questions ($\geq 70\%$) correct in order to pass while USC/WIAT users must obtain at least 19 out of 23 questions ($\geq 83\%$) correct in order to pass. Appendices A, B, and C provide a more comprehensive list of exam and course differences.

Training Domains and Mediums

The trend for organizations to train employees via some type of learning technology such as CBT is overwhelmingly apparent and predicted to continue.

However, organizations recognize that CBTs may not be enough to ingrain knowledge of particular importance. Information Assurance for IT-dependent organizations including the military is an especially critical subject area in which leaders must ensure personnel are properly knowledgeable and skillful. The overall name for the military instructional program under which network security training falls is the Information Assurance Education, Training, and Awareness (IA ETA) program. The IA ETA program covers a wide range of subsidiary information security and assurance programs. IA awareness is defined in AFI 33-204 as an “integrated communications awareness program” covering the divisions of information security (INFOSEC) such as communication security (COMSEC), computer security (COMPUSEC), and emissions security (EMSEC) (DAF, 2001: 2). An IA ETA program can be thought of as a single integrated program spanning the divisions of information security but also the learning phases of education, training, and awareness. The purpose of this next section of reviewed literature on IA ETA programs is to provide a background into instructional exposure strategies both within and beyond CBTs. The concept of awareness and training instruction beyond CBTs describes the construct of non-CBT instructional exposure.

Information Assurance Education, Training, and Awareness (IA ETA)

An IA ETA program accomplishes its aims through a broad instructional program that spans the learning continuum (Maconachy, 1989). All employees must first be made cognizant of the inherent value of information and of the various threats of information compromise through awareness efforts. Employees should learn how to perform existing procedural techniques through training efforts. Those employees working in the IA office or with high level access to sensitive information and information systems should

be instructed in the discipline of information assurance through education efforts. Each continuum phase of an IA ETA program should relate to and support formal organizational policy that is already in place.

Awareness

Awareness is the first phase of an IA ETA program and its least in-depth learning level. The awareness phase focuses on employees' short-term memories. Awareness efforts are generally aimed at broad audiences. Fundamental to awareness techniques are unique attention-grabbing methods intended to stimulate employees and get them thinking about information assurance and its associated issues (Maconachy, 1989, Thomson and Von Solms, 1998). Awareness activities for employees are mostly passive, as they are receivers of information through various messaging techniques that normally do not elicit employee interaction (Katsikas, 2000). Department of Defense instructions outline the goal of awareness as "heightening threat appreciation and the importance of adhering to protective measures" (DoD, 1997: A-8).

In today's business environment, all employees should be exposed to the awareness phase of an IA ETA program. All employees are information users, but are not necessarily system users. IA is applicable to both information and system users, because both groups are likely encounter valuable corporate information.

Awareness strategies occur across a broad spectrum of physical, paper, verbal, and electronic medium. Physical approaches include the use of promotional items like pens, coffee mugs, and letterhead with distinct logos and graphics containing catchy phrases. Paper-based techniques include posters, newsletters, articles, and distribution of IA formal policy documents. Verbal techniques at the awareness level include short

informative briefings and word-of-mouth campaigns ideally initiated from a central IA office through various departmental points of contact. Electronic strategies include screen savers, electronic bulletin board postings, videos, websites, and mass e-mails.

Awareness messages should originate from knowledgeable and impressive sources. Experts also state that the support of senior leadership in advocating the importance of IA cannot be understated (Desman, 2002; Maconachy, 1989; Spurling, 1995). All of these various awareness approaches should focus on conveying the inherent value of information, its risk of being compromised, the relevant consequences of compromise, and simple measures to prevent compromise. Successful awareness initiatives achieve an important transformation within employees by altering their attitudes toward the subject of Information Assurance (Catenazzo, 2000; DAF, 2001; USC, 2002).

Training

The next phase of the learning continuum within an IA ETA program is training. This is the level at which CBTs reside, but there are many other mediums that can be used for training employees. Training's main purpose is to "develop skills and abilities to mitigate system vulnerabilities, and implement and maintain protected systems" (DoD, 1997: A-8). As compared to awareness efforts, training sessions usually require more of an employee's time, are more formal in nature, and contain a much more active component (Katsikas, 2000, Maconachy, 1989). Training efforts are focused on the intermediate-term memory of employees (USC, 2002). Effective training environments should contain relatively small groups of employees (approximately 10-30 individuals) to allow adequate individualized instructor attention.

Small classroom instruction with individualized trainer attention is likely to positively affect an employee's development of information assurance skills. Realistic scenarios of potential information compromise incidents should be presented to employees. Specific and appropriate courses of action need to be learned and practiced during training. Role-playing exercises can aid in the acquisition of skills during training. Employees must understand how to act in applying information protection measures in a variety of environments. Adequate time should also be spent on information compromise scenarios such as the handling, storage and destruction of physical documents of a sensitive nature and the appropriate handling of information probing from outside sources. IA training sessions need to encompass all information exchange environments including the electronic and non-electronic domain.

The key at the training level is to avoid stale content and presentation techniques (Catenazzo, 2000). IA training programs should require employee participation and interaction. A standard military briefing is not sufficient at this level of learning. E-mailed briefings can also prove ineffective in attaining a high level of skill among employees. Although standardized procedures should be presented, training should be personalized and adaptable so as to remain relevant and interesting. The appropriate level of training required will vary among offices and employees and depend upon the level of exposure to information and information systems (Katsikas, 2000). This stresses the need for tailorable training programs. A way to streamline the management of training is to build the overall program in a modular fashion so sections can be easily added and subtracted as appropriate for the group being taught. This would result in the presentation of likely and actual information scenarios for that group, as well as make the

training relevant and allow employees to draw upon personal experience. Today's information-rich business environment beckons the need for some level of IA training among all employees. Employees not properly trained and made to understand information protection procedures place their company in a vulnerable position open for information compromise.

Education

The most complex phase of the learning continuum within an IA ETA program is education. Education aims at creating expertise and specialization within the field of IA and is focused on employees' long-term memory (Katsikas, 2000). Education adds a conceptual and theoretical basis to IA and aids employees in utilizing abstract thought in analyzing issues and situations, perhaps ones they have not encountered or been trained upon. Education is said to "provide the concepts and knowledge to develop appropriate technologies, policies, procedures, and operations to protect systems" and in a broader context than systems, information (DoD, 1997: A-8).

Employees educated in IA are called on to "perform operations such as analysis, evaluation, and judgment to reach higher cognitive level decisions which lead to the accommodation of newly integrated knowledge and skill" (Maconachy, 1989: 557G). In such a case, employees engage in complex self-instruction reached through personal interpretation and experience. IA education involves in-depth study and strives to achieve a fuller understanding of the subject matter. Employees formally educated in the discipline of IA should participate proactively in identifying and correcting vulnerabilities.

Education efforts include formal course-work at professional seminars and accredited institutions of higher learning at the undergraduate and graduate level. Education requires outside and background reading to allow interpretive learning to take place (USC, 2002). Following course preparation, this educational learning facilitates detailed discussions where students are expected to participate and provide personal analysis of the issues being reviewed.

Table 1 provides an expanded reference from USC (2002) of the instructional domains of awareness, training, and education, as well as an example of some teaching methods used within each domain. The expansions of the table were added by this author and are shown in italics. This study is aimed at assessing typical end-user instructional exposure and therefore focuses the construct of non-CBT instructional exposure on the domains of awareness and training. It has been noted that knowledge retention is affected by related instructional exposure (Wisher et al., 2001) and therefore is proposed that non-CBT instructional exposure related to NUL and USC/WIAT courses will positively affect knowledge retention.

**Table 1. Instructional Domains and Mediums: Training, Awareness, and Education
(Expanded from USC, 2002)**

	AWARENESS	TRAINING	EDUCATION
Attribute:	“What”	“How”	“Why”
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	<u>Media</u> - Videos - Newsletters - Posters - <i>Articles</i> - <i>Websites</i> - <i>Emails</i>	<u>Practical Instruction Method</u> - Lectures - Case Study - Workshops - Hands-on practice - <i>Computer SW</i> - <i>Computer-based training</i>	<u>Theoretical Instruction Method:</u> - Discussion Seminar - Background Reading - <i>Undergraduate and Graduate Degree Classes</i>
Test Measure:	- True/False - Multiple-choice (Identify learning)	Problem Solving (apply learning)	Essay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

Job Field and Other Demographics

This study will also explore possible effects of job field and other collected demographics on knowledge retention. It is proposed that individuals reporting communications as their job field will possess a higher level of baseline knowledge regarding the network security content of the NUL and USC/WIAT courses. This belief in a higher level of baseline knowledge is rooted in the assumption of a background in the communications field, either obtained through formal or informal schoolings as well as experience in the communications field to include aspects of network and information security. Because of this higher level of baseline knowledge, it is proposed that when compared to individuals in non-communications job fields, individuals in the

communications job field will exhibit higher levels of knowledge retention. It is also believed that communications job field individuals will be exposed to related instructional material beyond the NUL and USC/WIAT CBTs to a higher degree than those not in a communications job field. Therefore, it is proposed that communications job field individuals will exhibit higher levels of non-CBT instructional exposure than non-communications job field individuals. Other demographic effects on knowledge retention will also be explored to include: major command (MAJCOM), unit, employee category, and attained education level.

Hypotheses

The following hypotheses in Table 2 are based upon the reviewed and relevant literature. Hypotheses H1a and H2a provide specific user sample references and were made following the content analysis of the USC/WIAT and NUL CBT in Chapter IV (see Table 4). Figure 3 a graphical view of a synthesized research model derived from the hypotheses.

Table 2. Hypotheses

<p>H1: Overall interactivity will positively correlate with learning effectiveness, as measured by initial student performance (initial test score (T1)), therefore...</p> <p>H1a: Because of higher overall interactivity, NUL treatment group users will demonstrate higher levels of learning effectiveness (higher initial test scores (T1)) as compared to USC/WIAT treatment group users</p>
<p>H2: Overall interactivity will positively correlate with knowledge retention as measured by <i>relative retained knowledge</i>: [(retest score / initial test score) · 100] therefore...</p> <p>H2a: Because of higher overall interactivity, NUL treatment group users will demonstrate higher levels of knowledge retention as measured by relative retained knowledge as compared to USC/WIAT treatment group users</p>
<p>H3: Non-CBT instructional exposure level will positively correlate with knowledge retention as measured by relative retained knowledge</p>
<p>H4: Job field will have a significant effect on knowledge retention</p> <p>H4a: Users that report communications their job field will demonstrate a higher level of knowledge retention as measured by relative retained knowledge as compared to users who report a non-communications job field</p>
<p>H5: Job field will have significant effect on non-CBT instructional exposure level in that...</p> <p>H5a: Users that report communications as their job field will exhibit a higher non-CBT instructional exposure level than those that report a non-communications job field</p>
<p>Exploratory: Possible MAJCOM, unit, attained education level, or employee category trends affecting knowledge retention or non-CBT instructional exposure</p> <p>H6: These user demographics may/may not have a significant effect on knowledge retention</p>

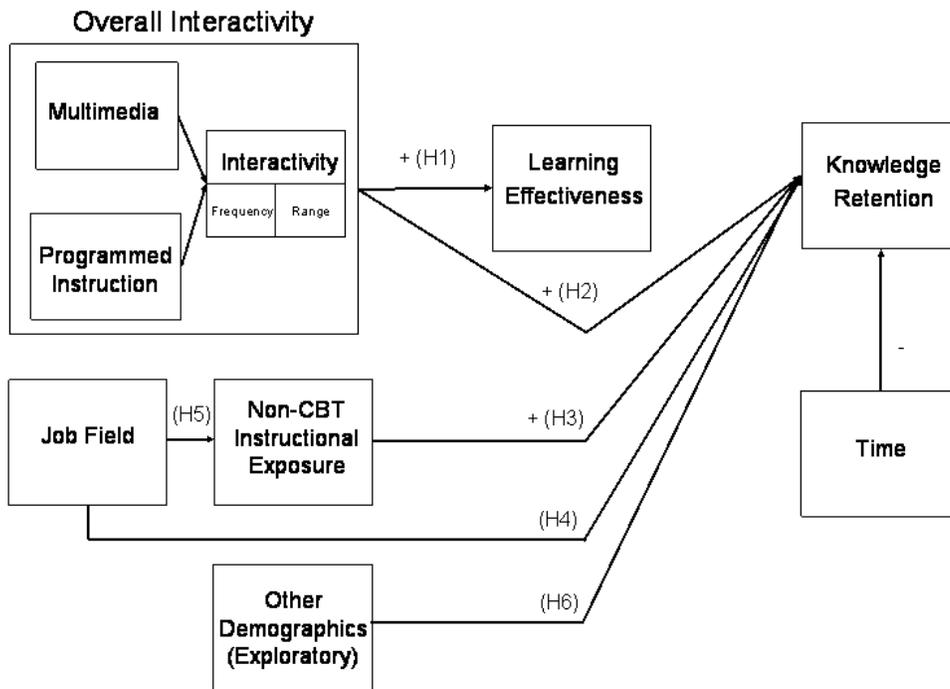


Figure 3. Synthesized Research Model

Summary

This chapter reviewed relevant literature in the areas of learning theories and teaching strategies specific to interactivity. An emphasis was put on learning in a computer-mediated environment such as CBT. A review of current and past research in the learning outcome areas of learning effectiveness and knowledge retention was covered. Discussed were the instructional domains and communication mediums outside CBT that organizations utilize to convey Information Assurance material to personnel. A background of the CBTs of interest, NUL and USC/WIAT, was covered. This chapter concluded with the proposal of several hypotheses. The next chapter will detail the methodology that was used in testing the proposed hypotheses.

III. Methodology

Overview

This chapter describes the methodology used in the preparation for, and measuring of, key constructs linked with the hypotheses set forward in Table 2 and present within the synthesized research model, Figure 3. Between the two CBTs of interest, NUL and USC/WIAT, the overall interactivity level is the prime design differentiator. However, as previously noted, each CBT's evaluation criterion (pass/fail threshold) for each test is considerably different ($\geq 70\%$ for NUL and $\geq 83\%$ for USC/WIAT). The independent components within overall interactivity studied are: multimedia, programmed instruction, frequency of interactivity, and range of interactivity. As previously discussed, the concept of instructional exposure describes the frequency by which individuals are exposed to non-CBT material related to information/network security. The constructs of learning effectiveness and knowledge retention were proposed to be dependent upon varying levels of overall interactivity (H1 and H2). Knowledge retention is also proposed to be dependent on non-CBT instructional exposure (H3). Certain subject demographics are also believed to have an effect on knowledge retention and non-CBT instructional exposure. One's job field is believed to have a significant effect on both knowledge retention (H4) and non-CBT instructional exposure (H5). Also explored is the possibility of knowledge retention trends among major commands, units, attained education, and employee category (officer, enlisted, government civilian, or government contractor) (H6).

Research Methodology

The first stage of this research methodology consisted of a content analysis of the level of interactivity present in the NUL and USC/WIAT CBT. This content analysis was used to determine the treatment differences as experienced by those subjects who indicated they first reviewed the CBT course prior to taking the initial exam.

The second stage of this study utilized two design strategies; quasi-experimental and survey. Both designs were merged and implemented into one web-based retest/survey assessment tool (Appendices D and E). These assessment tools were administered to both student sample groups (NUL and USC/WIAT). Both the NUL and USC/WIAT end-of-course exams were comprised of 23 multiple-choice questions - each with one correct answer and three distracters. The main differences between exams were a different question 8 (Appendices D and E) and different pass/fail thresholds. In order to provide the most exact comparison between test-retest within CBT user groups, the retest portion of the online assessment also contained a different question 8. For purposes of furthering IA training and awareness and providing individuals a gauge as to where they stand in reference to the desired performance score, it was decided to provide respondents with feedback on their performance on the retest portion of the online assessment.

The quasi-experimental design portion of this study was driven by methodologies found in academic literature that measured learning effectiveness and knowledge retention among students in both traditional classroom and CBT course environments. The survey design portion of this study was originally developed by this author for the purpose of measuring the concept of non-CBT IA instructional exposure. The

development of the survey portion of this study was grounded within practitioner literature, as well as DoD and USAF publications. The following sections go into more detail on the content analysis, quasi-experiment, and survey.

Interactivity Content Analysis, NUL and USC/WIAT

In order to accurately assess the poignant differences between the two CBTs, a content analysis of overall interactivity was performed. This author conducted a content analysis covering the four main components of overall interactivity: (1) multimedia, (2) programmed instruction, (3) frequency of interactivity, (4) range of interactivity. The classification system associated with the content analysis is shown in Figure 4 in the bottom portion of each construct box. The classification system was constructed in order to limit the amount of categories per construct and minimize subjectivity. For multimedia, the category was single, dual, or multi. Although multimedia suggests the use of more than two implemented media, neither CBT exhibited more than two types with USC/WIAT implementing text only (single) and NUL implementing text and line drawings (dual). For programmed instruction, the category was either *yes* (programmed instruction was implemented) or *no* (programmed instruction was not implemented). The frequency and range content analysis was based upon Kettanurak et al's (2001: 550) Interactivity Measurement Matrix previously discussed in Chapter II and shown in Figure 1. The frequency analysis involved a raw count of the number of instances a student had the opportunity to interact (provide input in some form/manner) with the CBT during the course and also considered course navigation control features. The range analysis involved a count of the number of input choices and a description of the range of

outcomes that may occur as a result of a student’s choices at each interaction opportunity, as well as a subjective description of the navigational range of choices.

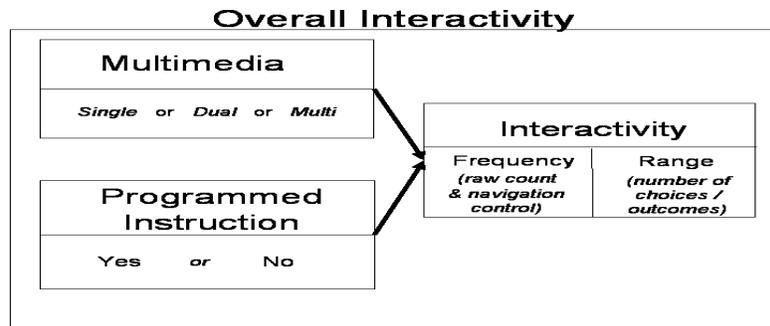


Figure 4. Overall Interactivity Content Analysis Methodology

Quasi-experimental component

In Dooley (2001: 349), a quasi-experimental design is described as an “experimental approach in which the researcher does not assign subjects to treatment and control conditions.” The quasi-experimental research design for this experiment is shown in Table 3.

Table 3. Quasi-experimental Design

	Archival / Initial	0-9 Month Retention Interval	Current
NUL Treatment Group	$X_a O_{1a}$	X_{Time}	O_{2a}
NUL Control Group	O_{1a}	X_{Time}	O_{2a}
USC/WIAT Treatment Group	$X_b O_{1b}$	X_{Time}	O_{2b}
USC/WIAT Control Group	O_{1b}	X_{Time}	O_{2b}

X_a = AFCA NUL CBT Course O_{1a} = AFCA NUL Initial Test O_{2a} = AFCA NUL Retest + Survey O_{1a} = O_{2a} Retest	X_b = WPAFB USC/WIAT CBT Course O_{1b} = WPAFB USC/WIAT Initial Test O_{2b} = WPAFB USC/WIAT Retest +Survey O_{1b} = O_{2b} Retest
--	---

X_a and X_b treatment difference is primarily in levels of CBT interactivity
 O_{1a} and O_{1b} are identical for 22 of 23 exam questions; difference is primarily in the pass/fail threshold ($\geq 70\%$ NUL, $\geq 83\%$ USC/WIAT)
 Treatment groups reported that they reviewed CBT courses prior to taking initial test
 Control groups reported that they did not review courses prior to taking initial test

The quasi-experimental portion of the web-based assessment was comprised of the 23 multiple-choice knowledge based questions found in Appendices D and E. Retests within the main student groups (NUL and USC/WIAT) were identical to their initial test in that they contained the same multiple-choice questions with the same one correct answer and the same three distracters. This experiment consisted of four subject groupings: (1) AFCA NUL treatment group (reported that they reviewed NUL course before taking initial test), (2) AFCA NUL control group (reported that they did not review NUL course before initial test), (3) WPAFB USC/WIAT treatment group (reported that they reviewed USC/WIAT course before taking initial test), and (4) WPAFB USC/WIAT control group (reported that they did not review USC/WIAT course before taking initial test).

Due to the fact that an individual needs only to take one of the courses to satisfy the network-user training requirement, it is assumed that USC/WIAT users did not review the NUL course (X_a) prior to their initial test and that NUL users did not review the USC/WIAT course (X_b) prior to their initial test (Table 3). This author had no control over which individuals were assigned to which treatment group, hence the designation of this component of the assessment as quasi-experimental. Of important note is that the Air Force has been using similar course and test material present in both CBTs for a number of years. This leads to the realization that users in all treatment groupings may have viewed either CBT course or similar training material in previous years. The test/retest design lends itself to a certain amount of invalidity, in that all subject groups have previously taken the initial test and the retest may be measuring their ability to recall exam-specific knowledge such as question and answers. This situation

may interfere with the retest's ability to measure true knowledge retention levels.

Without the ability to assess subject knowledge levels prior to taking the course or initial test, a baseline level of knowledge for each subject grouping was unable to be assessed.

Both CBTs have their own information gathering databases (DB), which track student information by course. Each DB records certain demographic and course-specific data such as email and initial test date. Observations O_{1a} and O_{1b} represent a student's initial (archival) test score percentage and were recorded by the DBs (Table 3). Therefore, it must be noted that the archival segment of data for both samples was independently collected prior to undertaking this study and without the involvement of this researcher.

As discussed in Chapter II, the learning effectiveness of a training program is consistently measured by student performance/achievement as assessed by some type of overall end-of-course test (Fletcher, 1996; Johnston, 1995; Kulik and Kulik, 1991; Niemiec and Walberg, 1987). The end-of-course test correlates with the initial tests taken at O_{1a} and O_{1b} for NUL and USC/WIAT users respectively (Table 3). Analysis of learning effectiveness for each CBT was conducted using standard measures of central tendency and variance. Learning effectiveness differences between NUL and USC/WIAT users is the focus of Hypothesis 1.

Throughout academic literature, knowledge retention has consistently been measured by the amount of course material recalled by students who previously completed a training course. Knowledge retention studies have typically used uniform follow-up intervals (all subjects were retested X amount of time following initial end-of-course test). This study differs in design in that knowledge retention is measured across

various follow-up intervals ranging from 0 to 9 months. As mentioned in Chapter II, knowledge retention is operationalized as *relative retained knowledge*, defined as performance on a retention exam relative to performance on an initial exam, and has a formula of: $[(T2/T1) \cdot 100]$. Knowledge retention analyses performed in this study used the relative retained knowledge formula and reference time by either number of days passed since initial test or by parsing users in month groups.

Survey component

As Wisner et al. (2001) and others have noted, learning and practice outside initial training and during the retention interval could directly affect knowledge retention. For this reason, an original survey component was developed in order to ascertain the level to which individuals received learning and practice related to network and information security issues. This original survey component is contained in the second portion of this study's web-based assessment. The survey section is comprised of 12 medium-specific questions and 1 non-medium-specific question dealing with how often individuals are exposed to network/information security issues in non-CBT mediums.

The purpose of the survey segment was to assess the degree to which a subject experienced non-CBT IA instructional exposure - a central measure to Hypothesis 3. This survey segment contained 13 questions with a seven-item response scale containing the time frequency choices of: never, annually, bi-annually, quarterly, monthly, weekly, and daily. Subjects were forced to choose just one time frequency for each question. The survey segment can be found in the tabled section following the multiple-choice questions in Appendices D and E. The 13 survey questions all had equal answer scales and differed only in the non-CBT medium in which they inquired about. The mediums

inquired about were derived from a synthesis of academic, practitioner, and government publications dealing with non-subject specific and IA-subject specific education, training, and awareness domains and mediums (Catenazzo, 2000; DAF, 2001; Desman, 2002; DoD, 1997; Katsikas, 2000; Maconachy, 1989; Spurling, 1995; Thomson and Von Solms, 1998; USC, 2002). The mediums inquired about can be found in Table 1 of Chapter II titled Instructional Domains and Mediums, Training, Awareness, and Education and are derived and expanded from USC (2002).

In order to provide some measure of reliability within the non-CBT instructional exposure (NIE) survey section, a question was added to the demographic section of the web-based assessment (Appendices D and E, question 7). This question asked subjects, “Do you work with Network / Information Security issues on a regular basis (weekly)?” Subjects were given a dichotomous answer choice of *yes* or *no*. Subjects who worked with network/information security issues at least on a weekly basis are expected to answer “yes.” A similar broad-based exposure question was located as question *m* in the NIE survey and was worded as follows, “Considering all of the above mediums and others not mentioned, how often are you exposed to network / information security issues?” Subjects in this instance were given 7 choices of frequencies ranging from daily through never. Subjects who had previously reported *yes* to question 7 in the demographics would be expected to answer either *weekly* or *daily* for question *m*, while subjects who had previously reported *no* to question 7 would be expected to not answer with either *weekly* or *daily*. It must be noted that although these two questions attempt to assess some overall measure of instructional exposure, they are not meant to measure the exact same phenomenon, just a similar one.

Pilot Study

A pilot study of each CBT-specific assessment tool was conducted on network end-users at the Air Force Institute of Technology (AFIT). Forty-one total subjects participated in the pilot study; fifteen for the NUL assessment version and twenty-six for the USC/WIAT version. Each participant was an active-duty company grade officer enrolled in a graduate program at AFIT. The pilot study was used to evaluate assessment tool readability, clarity, grammar, ease of navigation, and comprehension of the non-CBT instructional exposure survey section. Pilot participant feedback on readability, grammar, and navigation was aggregated and incorporated into the final version of each assessment tool. Pilot study subjects also indicated a full understanding of the non-CBT instructional exposure survey section leading to confidence that this section would measure what it was set out to measure. The conduction of the pilot study resulted in refined and more valid research instruments.

Population

The true population of interest for this study is all AF network end-users. This population includes, but is not limited to, all military members, government civilians, government contractors, AF Academy cadets, and local and foreign nationals. Assuming the vast majority of AF personnel are network end-users, the latest AFPC statistics estimate the size of this population in excess of one-million individuals. However, because of a lack of central management, data from all these individuals was not available for sampling. The sub-population sets used were (1) network end-users AF-wide that took the AFCA NUL CBT (the de facto AF standard) and (2) network end-users local to WPAFB that took the WPAFB USC/WIAT CBT. Using these two

subpopulation sets gave this research study the broadest available view of AF network end-users.

Subjects

This study was conducted in December 2002. Actual subjects in this study were Air Force network end-users currently authorized and licensed to utilize AF networks. Therefore, AFI-33-115v2 would dictate that all subjects had previously demonstrated some acceptable level of competency in network security material. Subjects included military (enlisted and officer), government civilian, and government contractors.

Records from each CBTs DB were used to obtain potential subjects. A subject's last method for obtaining network user licensing was used as the designator of a subject's primary group placement (NUL or USC/WIAT). Since retraining network end-users is currently set as an annual requirement, it was assumed that records older than one year represented subjects who had already been retrained. Therefore archival data records older than one year (prior to January 2002) were discarded. To qualify as a potential subject for this experiment, one had to meet all of the following prerequisites:

1. Subject was an Air Force network end-user,
2. Subject had previously completed the AFCA NUL CBT or WPAFB USC/WIAT CBT between the months of January and November 2002, *and*
3. Subject had provided a valid email address to the NUL or USC/WIAT course management systems.

The range of available archival data of interest from each CBT's course management system differed. For the larger subpopulation set (NUL), a significant set of

archival data records were available from April through November 8, 2002. USC/WIAT archival data was available from January through October 13, 2002. In an attempt to obtain similar retest time-passed distributions, sampling was made from users that had enrolled and completed either CBT between April and November 2002.

Sampling of Archival Records

Sampling techniques were done individually from each set of archival records. Due to a high variance between the number of participants from each month group and the desire to achieve equal representation of retention interval groups, archival records were first divided into month groups (Apr 2002, May 2002...). It was from these month groups that subjects were randomly sampled. NUL archival records that met the previously outlined subject prerequisites totaled 24,762 users spread unevenly across month groups from April through November 2002. USC/WIAT archival records that met the previously outlined subject prerequisites totaled 7,516 users spread somewhat evenly across month groups from April through October 2002. Expectations were for a response rate of approximately 30%. Since a sample size of 1,000 per CBT group was desired, 500 USC/WIAT users were sampled from each month (3,500 total) and 450 NUL users were sampled from each month (3,600 total).

Participant Solicitation and Navigation of Web-based Assessment

Individual emails originating from an organizational email account were sent to the 7,100 randomly sampled users. Emails varied slightly, depending upon the CBT group with which the recipient was previously identified. A generic version of the solicitation email is located in Appendix F. Each email contained a brief summary of the research objectives, their importance to AF network security, and the particular reason

each potential subject had been chosen. Each email also contained a link to an Internet-based webpage that contained the appropriate web-based assessment. If users chose to participate, they would click on the provided link and be brought to webpage 1 of 3 (Appendices D and E, page 1). This webpage provided directions on how to complete the survey, an anonymity statement, a contact email address, and provided for demographic-type user input. Page 1 included both open-ended input instances (email, unit, and Air Force Specialty Code) and drop-down input instances (MAJCOM, employee category, job field, education level) (Appendices D and E, page 1). Page 1, question 9, asked specifically whether or not subjects had first reviewed their respective CBT courses prior to taking the exams (Appendices D and E, page 1). The reported answer to this question determined a subject's treatment group assignment in that those that reported they had first reviewed the CBT course prior to taking the exam were placed in the treatment groups and those that indicated they had not reviewed the CBT course prior to taking the exam were placed in the control groups.

Following the completion of page 1, users would click on a "continue" action button and be taken to page 2, which contained the knowledge-based retest and non-CBT instructional exposure survey portion of the assessment, as well as section-specific directions (Appendices D and E, page 2). Subjects were given directions to use only the knowledge in their memories without the aid of any supplemental material in answering the test portion of the assessment. Page 2 also allowed users the opportunity to provide open-ended feedback regarding the CBT they had previously taken and their local network and information security training and awareness program. Following completion of all page 2 inputs, users would click on the "Submit Survey" action button.

This action took users to page 3, which gave them feedback on their performance on the knowledge-based retest section of page 2 (Appendices D and E, page 3). Users were provided with the number of correct answers as well as a “passing” or “failing” mark dependent on the setting of their particular CBT’s pass/fail threshold ($\geq 70\%$ or ≥ 16 correct answers for NUL and $\geq 83\%$ or ≥ 19 correct answers for USC/WIAT).

Usable Sample Prerequisites

In order to use only valid subject data, certain usable sample prerequisites were set. The main qualifier was that users had to complete the survey in its entirety. Measurement of the knowledge retention construct requires the data of both a subject’s initial test date and initial test score. In order to link a subject’s new data record with the corresponding archival data record, the email input from page 1 of each web-based assessment was used to uniquely identify an individual and join new and old test data. If the subject did not provide a valid email address on page 1, the new record was discarded. If there was no match in the archival record, the new record was also discarded. In summary, the following usable sample prerequisites were set:

1. Subject had to complete the web-based assessment in its entirety,
2. Subject had to provide a valid email address on page 1,
3. NUL subject’s provided email address could be matched to an email address in the archival NUL records *or*
USC/WIAT subject’s provided email address could be matched to an email address in the archival USC/WIAT records.

Statistical Analyses, Planned

Statistical techniques planned for use in this study were: independent sample t-tests, analysis of variance (ANOVA), simple linear regression, and multiple linear regression.

Summary

This chapter described the overall methodology of this study. The research methodology and design was reviewed. Central to research methodology and design were the proposed hypotheses set forth in Chapter II. Characteristics of the population of interest were noted along with controlled and uncontrolled parameters associated with the sample. The sampling technique, participant solicitation, web-based assessment navigation, and usable sample prerequisites were also outlined. The results of statistical analyses are reported in Chapter IV and include hypothesis testing, as well as practitioner-oriented analyses. Chapter V will contain discussions and conclusions drawn from the analyses, limitations of this study, as well as academic and practitioner implications of the findings.

IV. Analysis

Overview

This chapter presents the results of analyzing the data sets collected through the implementation of the research design. First presented is the interactivity content analysis that was critical in assessing the treatment differences between the NUL and USC/WIAT CBTs. This is followed by a section describing the steps taken in determining usable web-based assessments as well as the demographic makeup of the two usable sample sets. The main part of this chapter presents analyses pertinent and specific to the six hypotheses proposed in Table 2 of Chapter II. Also presented are the procedures for calculating construct measurements as well as reliability calculations for the construct of non-CBT instructional exposure. This chapter includes additional analyses relevant for practitioner/managerial use. This chapter attempts to objectively present the results of the analyses. Discussion of the findings and implications thereof is contained in Chapter V.

Interactivity Content Analysis

Table 4 below represents the results of the interactivity content analysis performed by this author and based upon the interactivity assessment framework in Figure 4 of Chapter III. This framework included an analysis of the four components of *overall interactivity*: frequency, range, multimedia, and programmed instruction.

Table 4. Interactivity Content Analysis, Results

	AFCA NUL	WPAFB USC/WIAT
<i>Frequency</i>	9 embedded questions, Navigation control feature, <u>LOW</u>	ZERO opportunities for input during course <u>NONE</u>
<i>Range</i>	Choose 1 or more of 4 possible answers (Feedback varies depending on right or wrong answer), Navigate directly to any of the 5 sections of the course and the course test <u>LOW</u>	Null (No input, therefore no range) <u>NONE</u>
<i>Multimedia</i>	Dual (Text and Graphics)	Single (Text only)
<i>Programmed Instruction</i>	Yes	No
<i>OVERALL INTERACTIVITY</i>	LOW	NONE

As shown, the interactivity content analysis resulted in an overall interactivity assessment of *LOW* for the NUL CBT and *NONE* for the USC/WIAT CBT, whereas there is no interactivity believed to be present within the USC/WIAT CBT. The single media text of the USC/WIAT CBT can be likened to no more than a *plain* online text book and as such is believed to have a negligible effect on interactivity.

Sampling Results

Per the usable sample prerequisites outlined in Chapter III, filtering of web-based assessment responses was performed as shown in Table 5.

Table 5. Sampling Results

NUL web-based assessments	USC/WIAT web-based assessments
<p>517 total responses <u>minus</u></p> <p>↓</p> <p>115 incomplete responses <u>minus</u></p> <p>↓</p> <p>36 unmatched / invalid emails <u>minus</u></p> <p>↓</p> <p>6 records in the 8-9 month group (this excision was performed because the sample size at this retention interval was insufficient) <u>resulting in</u></p> <p>↓</p> <p>360 NUL records (13% usable response rate)</p>	<p>569 total responses <u>minus</u></p> <p>↓</p> <p>118 incomplete responses <u>minus</u></p> <p>↓</p> <p>67 unmatched / invalid emails <u>resulting in</u></p> <p>↓</p> <p>384 USC/WIAT records (15% usable response rate)</p>

For each sub-sample, not all email solicitations resulted in successful delivery. The usable response rate was calculated from the total emails successfully delivered to each sub-sample. The number of successful email deliveries for NUL users was 2,784 and for USC/WIAT users was 2,600 (5,384 total successful email deliveries out of 7,100 total email solicitations).

In order to assess the demographic makeup of the sample sets, an analysis was performed. The sample sets were shown to be extremely diverse in their makeup as follows:

Table 6. Sample Demographics

NUL sample users (n = 360)	USC/WIAT sample users (n = 384)
1-8 months from initial training	2-9 months from initial training
All 9 Major Commands (ACC, AETC, AFMC, AFRC, AFSOC, AFSPC, AMC, PACAF, USAFE)	278 separate office symbols with 6 major WPAFB units highly represented (445 AW, 74 MDG, 88 ABW, AFRL, ASC, HQ AFMC)
<p><u>293 total military</u> 240 Enlisted (E-2 to E-9) 53 Officers (O-1 to O-6)</p> <p>55 Government Civilians and 12 Government Contractors</p>	<p><u>131 total military</u> 50 Enlisted (E-2 to E-9) 81 Officers (O-1 to O-10)</p> <p>174 Government Civilians, 77 Government Contractors, and 2 Other</p>
15 different Job Fields (35% Communications)	15 different Job Fields (5% Communications)
All Attained Education Levels Represented	All Attained Education Levels Represented
	As an AFMC-dominated base, vast majority (84.3%) reported AFMC as major command

ACC - Air Combat Command
AETC – Air Education and Training Command
AFMC – Air Force Materiel Command
AFRC – Air Force Reserve Command
AFSOC – Air Force Special Operations Command
AFSPC – Air Force Space Command
AMC – Air Mobility Command
PACAF – Pacific Air Forces
USAFE – United States Air Forces in Europe

445 AW – 445th Airlift Wing
74 MDG – 74th Medical Group
88 ABW – 88th Air Base Wing
AFRL – Air Force Research Laboratory
ASC – Aeronautical Systems Center
HQ AFMC – Headquarters Air Force Materiel
Command

Construct Measurement Formulas

The following table describes the constructs contained within the proposed hypotheses, their predictive/postdictive position in the research model, their data category, and the formula or determination method used in calculating data values for each construct.

Table 7. Construct Measurement Formulas

<u>Construct</u>	<u>Independent / Dependent</u>	<u>Data Category</u>	<u>Formula / Determination</u>
Overall Interactivity	Independent	Ordinal	Content Analysis derived from components in Figure 4, Chapter III Values of NONE, LOW, MEDIUM, or HIGH
Learning Effectiveness	Dependent	Continuous	Initial/Archival Test Percentage Score (T1) $T1 = [(\# \text{ correct} / \text{total } \# (23)) \cdot 100]$
Knowledge Retention	Dependent	Continuous	Relative Retained Knowledge: $(T2 / T1) \cdot 100$
Non-CBT Instructional Exposure (NIE)	Independent and Dependent	Ordinal / Continuous	(1) (Ordinal) Reported frequency (daily, weekly, etc.) (2) (Continuous) Recoded and non-CBT IE Weighted Average (NIEWA) calculated from survey questions a through l Formula = $[\text{SUM} (1 \cdot (\text{posters, emails, videos, newsletters, articles, military websites, non-military websites}) + 2 \cdot (\text{lectures, workshops}) + 1.5 \cdot (\text{computer software, senior leaders}) + 2.5 \cdot (\text{practice})) / 12]$ *Formula 2 used in MLR
Job Field	Independent	Nominal	Subject-reported: communications / flying operations / medical / etc. Recoded as two-levels: (1) communications and (2) non-communications
Exploratory Demographics	Independent	Nominal	Subject-reported - MAJCOM (AETC, AFSPC, etc.) - Education (HS, AD, BD, MD, PhD) - Unit (AFRL, AFIT, ASC, etc.) - Employee Category (Enlisted, Officer, Govt Civilian, Govt Contractor)
Time	Independent	Continuous	Number of Days Passed since initial/archival test (T1)

The key facet of the above table is the formula/determination column. Several of the constructs formulas are self-explanatory and have been previously discussed. However, non-CBT Instructional Exposure (NIE) and its formula for a weighted average have not been discussed. As mentioned, the NIE survey portion of the web-based assessment allowed subjects to enter one of seven frequency choices ranging from never to daily for all 12 medium-specific and the 1 non-medium-specific questions. In order to compute the non-CBT instructional exposure weighted average (NIEWA), the data for the medium-specific questions was recoded from its ordinal value (never, annually, bi-annually, etc.) to a continuous value relative to the number of occurrences in a one-year period. The recoding scheme is shown below in table 8.

Table 8. Non-CBT Instructional Exposure Recoding Scheme

Ordinal Value	Recoded Continuous Value
never	0
annually	1
bi-annually	2
quarterly	4
monthly	12
weekly	52
daily	365

The next step in computing the NIEWA was to appoint weighted factor values to each medium. Table 9 below displays the weightings that were applied to each medium as relative to their associated memory level effect and as gleaned from Table 1, Chapter II: Instructional Domains and Mediums. For certain mediums, the weightings are derived from this author's subjective analysis of memory level effect, which considered multimedia use and the perceived level of interaction associated with each medium.

Table 9. Non-CBT Instructional Exposure Medium-Specific Weighting

Medium	Memory Level Effect	Weighted Factor
posters	short-term	1
emails	short-term	1
videos	short-term	1
newsletters	short-term	1
articles	short-term	1
military websites	short-term	1
non-military websites	short-term	1
computer software	short / intermediate-term	1.5
senior leaders	short / intermediate-term	1.5
lectures	intermediate-term	2
workshops	intermediate-term	2
hands on practice	intermediate / long term	2.5

As shown, those mediums with an associated longer memory level effect were assigned a higher weighted factor. The use of a weighted formula was chosen over an unweighted one because the effect of non-CBT instructional exposure on knowledge retention was the main construct relationship being explored. A weighted formula attempts to account for a varying degree of knowledge imprint capability between the different mediums. The actual formula used to compute the NIEWA was comprised of the (sum of the medium-specific recoded continuous values multiplied individually by their associated weighted factor) divided by (the total number of questions which was 12). The NIEWA formula in a simplified form is shown below in Equation 1 as follows:

Equation 1. Non-CBT Instructional Exposure Weighted Average (NIEWA)

$$NIEWA = [((1) \cdot (posters + emails + videos + newsletters + articles + military websites + non-military websites)) + ((1.5) \cdot (computer software + senior leaders)) + ((2) \cdot (lectures + workshops)) + ((2.5) \cdot (hands on practice))] / 12$$

Non-CBT Instructional Exposure (NIE) Survey Reliability

As discussed in Chapter III, two questions of a similar nature were asked in an attempt to provide some level of internal consistency within the NIE survey. A rudimentary correspondence analysis between question 7 and question m within individual surveys was conducted with the results as follows:

Table 10. NIE Correspondence Analysis

Evidence <u>for</u> relationship between questions	Evidence <u>against</u> relationship between questions
$\underline{27.57\%}$ Question 7 “yes” AND Question m “weekly” OR “daily”	$\underline{12.76\%}$ Question 7 “yes” AND Question m NOT “weekly” OR NOT “daily”
$\underline{34.27\%}$ Question 7 “no” AND Question m NOT “weekly” OR NOT “daily”	$\underline{25.4\%}$ Question 7 “no” AND Question m “weekly” OR “daily”
61.84% total <u>for</u> relationship	38.16% total <u>against</u> relationship

As shown, the analyses demonstrate some level of internal consistency among user responses to the survey questions measuring the construct of non-CBT instructional exposure. As previously noted in Chapter III, questions 7 and m do not measure the exact phenomenon, just a similar one.

Statistical Analyses, Actual

The statistical software package used for a large portion of statistical analyses was JMP (release 5.0). The mathematical software package MathCad version 2001i was also used in some analyses.

Statistical techniques employed in this study included: independent sample t-tests in both equal and unequal variances form, traditional analysis of variance (ANOVA), Welch ANOVA for unequal variance samples, simple linear regression, and multiple

linear regression. The assumptions associated with each statistical analysis, such as normality and equal variances for traditional t-test and ANOVAs, were tested for in each group comparison. The Welch and unequal variance t-tests were utilized when appropriate to account for unequal variances between groups. The Welch ANOVA method for means is based on the usual ANOVA F-test; however, the means have been weighted by the reciprocal of the sample variances of the group means (Welch, 1951). In the case of unequal variances, the Welch statistic results in a more conservative F statistic and pvalue, thereby providing a higher threshold for null hypothesis rejection. If there are only two qualitative levels, the Welch ANOVA is equivalent to an unequal variance t-test. When applied, the use of the Welch or unequal variance t-test over traditional methods is stated within the results.

Learning Effectiveness and Knowledge Retention, Entire Sample Set

In order to provide an overall view of learning effectiveness and knowledge retention across the entire sample set, independent analyses were performed on each sample group to assess learning effects over time. Table 11 below includes all sample groups whereas the NUL retention intervals span 1-8 months and the USC/WIAT retention intervals span 2-9 months.

**Table 11. Learning Effectiveness and Knowledge Retention
Among All Sample Groups and Across All Retention Intervals**

Sample Group	Initial Test Score Percentage (T1) (Learning Effectiveness)	New Test Score Percentage (T2)	Relative Retained Knowledge (Knowledge Retention) (T2 / T1) · 100	Relative Knowledge Loss [(T1-T2) / T1] · 100
NUL Control n = 108				
Mean	89.6	79.1	88.9	11.1
Median	91	78	87.4	12.63
Std Dev	9.2	10.9	13.7	13.7
P/F (≥ 70%)	100% / 0%	85% / 15%		
P/F (≥83%)	73% / 27%	43% / 57%		
NUL Treatment n = 252				
Mean	89.1	78.6	88.8	11.2
Median	91	78	90.7	9.3
Std Dev	8.2	11.3	14.2	14
P/F (≥ 70%)	99.996% / 0.004%	85% / 15%		
P/F (≥83%)	71% / 29%	45% / 55%		
USC/WIAT Control n = 70				
Mean	96.1	77.8	81.1	18.9
Median	100	78	83	17
Std Dev	5.6	13.6	14.2	14.2
P/F (≥ 70%)	100% / 0%	79% / 21%		
P/F (≥83%)	100% / 0%	49% / 51%		
USC/WIAT Treatment n = 314				
Mean	96.7	82.4	85.3	14.7
Median	100	83	87	13
Std Dev	4.8	10.7	11.2	11.2
P/F (≥ 70%)	100% / 0%	91% / 9%		
P/F (≥83%)	100% / 0%	60% / 40%		

<p>*All Mean, Median, and Std Dev values represent percentages P/F = Pass / Fail Threshold</p>
--

Table 11 addresses the relative knowledge loss. It is also important to address the raw knowledge loss, as measured by the difference between T1 and T2. Raw knowledge loss analysis between treatment groups is shown in Table 12 below.

Table 12. Raw Knowledge Loss Analysis, (T1 - T2)

Sample Group	Raw Percent Loss
NUL Control, n = 108	
Mean	10.6
Std Dev	12.7
NUL Treatment, n = 252	
Mean	10.5
Std Dev	13.0
USC/WIAT Control, n = 70	
Mean	18.3
Std Dev	14.0
USC/WIAT Treatment, n = 314	
Mean	14.3
Std Dev	10.9

It is noted that for each treatment group the raw percent loss is slightly larger than the relative percent loss values. On the 23 question tests used in this study, each 4-5% raw percent loss represents 1 additional incorrect answer. For example, 17 out of 23 correct results in a 74% while 16 out of 23 correct results in a 70%.

Hypotheses Testing

This section of the data analysis deals with statistical analyses specific to the hypothesized relationships among the constructs of interactivity, learning effectiveness, knowledge retention, non-CBT instructional exposure, and the demographics of job field, major command (MAJCOM), unit, employee category, and attained education.

Hypotheses 1, Overall Interactivity and Learning Effectiveness

Hypothesis 1 proposed a positive relationship between overall interactivity and learning effectiveness, as measured by initial test score. Per the CBT interactivity content analysis, the NUL course was found to have a higher level of interactivity. Therefore, hypothesis 1a proposed higher learning effectiveness in the NUL treatment group. In order to test for this directional hypothesis, a one-tailed t-test was used. The results of hypothesis 1 analysis are presented below in Table 13.

**Table 13. Hypothesis 1:
Effects of Overall Interactivity on Learning Effectiveness,
Treatment Group Analysis**

Sample Group	Initial Test Score Percentage (T1) (Learning Effectiveness)	t-stat (unequal variances)	One-tailed t-test $\alpha = 0.05$	pvalue
NUL Treatment n = 252	Mean = 89.1 Median = 91 Std Dev = 8.2 Skewness = -0.33 (Left)	-12.9 (u)	t critical = 1.648	< 0.0001
USC/WIAT Treatment n = 314	Mean = 96.7 Median = 100 Std Dev = 4.8. Skewness = -1.5 (Left)		Two-tailed t-test t critical = +/- 1.648	< 0.0001

* Significantly higher initial test scores for USC/WAIT Treatment group was found
(u) Indicates unequal variance t-test used

The one-tailed t-test performed from Table 13 data provides no support for H1, in that there is no statistical significance that the NUL Treatment group (higher

interactivity) exhibited higher initial test scores (learning effectiveness). However, a plain look at the measures of central tendency leads one to speculate about significance in the other direction. Therefore, a two-tailed t-test was performed, and it is shown that the USC/WIAT treatment group (no interactivity) exhibited statistically significantly higher initial test scores (learning effectiveness). It is noted that the distributions of initial test score for both treatment groups deviate from normality, with both groups exhibiting a left skewness. The deviation from equal variances was dealt with by using an unequal variance t-test. However, North Western University (NWU) (2003) notes that “if the sample sizes are approximately equal, and not too small, then the t statistic will not be much affected even if the population distributions are skewed, as long they have approximately the same skewness.” The sample sizes are approximately equal for the groups (252 and 314) and both are skewed left fairly heavily. Therefore, the effect of non-normality on the t-test is accepted as not radically altering its robustness.

Time and Knowledge Retention

Although not specifically hypothesized, the negative effect of time on knowledge retention has been cited throughout literature and exhibited across various academic studies. In order to test this relationship of time and knowledge retention in this study, a simple linear regression (SLR) analysis between time (days passed) and knowledge retention (relative retained knowledge) was performed among sample and aggregated sample groupings. The results of that analysis are found in Table 14 below:

Table 14. Time Effect (Days Passed) on Knowledge Retention (Relative Retained Knowledge) using SLR and single parameter t-tests

Sample Group	r ²	Days passed t-stat	One-tailed t-critical	pvalue
NUL Treatment n = 252	0.048	-3.57	-1.285	0.0004
USC/WIAT Treatment n = 314	0.01	-1.78	-1.284	0.0756
Both Treatment n = 566	0.032	-4.33	-1.283	< 0.0001
NUL Treatment and Control n = 360	0.043	-3.99	-1.284	< 0.0001
USC/WIAT Treatment and Control n = 384	0.018	-2.67	-1.284	0.0079
ALL groups including control n = 744	0.039	-5.5	-1.283	< 0.0001

*Using an Alpha of 0.1, all values convey a significant negative effect of time on knowledge retention, as measured by relative retained knowledge

The one-tailed t-test performed for each sample grouping indicates that there is a significant negative relationship between time and knowledge retention. The SLR analysis produces linear equations for each sample grouping. These equations represent mathematical functions which attempt to estimate the value of relative retained knowledge, $E(y)$, from the single parameter of days passed (X_1). The basic linear formula for a single quantitative parameter such as days passed is given in Equation 2 as follows:

Equation 2. Basic Simple Linear Regression Formula for Single Quantitative Parameter

$$E(y) = \beta_0 + \beta_1 X_1 + \varepsilon$$

In Equation 2 above, β_0 represents the y-intercept, β_1 represents the slope associated with parameter X_1 , and ε represents random error. The linear equations, minus the error term,

produced from the SLR analyses for relative retained knowledge in each sample grouping are given in Table 15 as follows:

Table 15. Linear Equations for Relative Retained Knowledge by Days Passed

Sample Group	Linear Equation
NUL Treatment	$E (\text{Relative Retained}) = 95.2 - (0.05 \cdot \text{Days Passed})$
USC/WIAT Treatment	$E (\text{Relative Retained}) = 88.1 - (0.02 \cdot \text{Days Passed})$
Both Treatment	$E (\text{Relative Retained}) = 92.0 - (0.04 \cdot \text{Days Passed})$
NUL Treatment and Control	$E (\text{Relative Retained}) = 94.9 - (0.04 \cdot \text{Days Passed})$
USC/WIAT Treatment and Control	$E (\text{Relative Retained}) = 88.6 - (0.03 \cdot \text{Days Passed})$
<i>ALL groups including control</i>	$E (\text{Relative Retained}) = 92.5 - (0.04 \cdot \text{Days Passed})$

The associated negative β_1 days passed slope values in the linear equations given above demonstrate that for each one day that passes, the estimate for relative retained knowledge drops from between 0.02% to 0.05% depending upon sample grouping.

Hypothesis 2, Overall Interactivity and Knowledge Retention

In order to determine the effects of overall interactivity on knowledge retention, values for new test score percentage, relative retained knowledge, and relative knowledge loss were computed for each treatment group (NUL treatment and USC/WIAT treatment). It is appropriate to use just the treatment groups since it is only these groups which experienced different levels of overall interactivity. In an attempt to compare similar retention intervals, the data sets were parsed into month groups, where each group spanned a one-month period ranging from 1-2 months to 8-9 months. The result of this analysis is contained in Table 16.

Table 16. New Test Score, Knowledge Retention, and Knowledge Loss Measures within Month Group Retention Intervals

Retention Interval	New Test Score Percentage (T2)		Relative Retained Knowledge (Knowledge Retention) $(T2/T1) \cdot 100$		** Relative Knowledge Loss $[(T1 - T2) / T1] \cdot 100$	
	NUL T	USC/WIAT T	NUL T	USC/WIAT T	NUL T	USC/WIAT T
1-2 mos	n = 42					
Mean	83.6		95		5	
Median	83		96.1		3.9	
Std Dev	10.4		11.4		11.4	
2-3 mos	n = 45	n = 74				
Mean	82	85.3	91.8	86.7	8.2	13.3
Median	83	87	91.6	87	8.4	13
Std Dev	11.4	10.3	13.2	10.9	13.2	10.9
3-4 mos	n = 23	n = 54				
Mean	79.7	82.3	90.5	85.9	9.5	14.1
Median	78	83	90.7	86.1	9.3	13.9
Std Dev	11.6	10.4	13.7	10.9	13.7	10.9
4-5 mos	n = 49	n = 37				
Mean	75.6	82.7	85.2	85.6	14.8	14.4
Median	78	87	87.4	87	12.6	13
Std Dev	11.5	10.5	15.2	9.5	15.2	9.5
5-6 mos	n = 32	n = 39				
Mean	74.4	83.9	84.9	86.6	15.1	13.4
Median	76	83	86.23	86.8	13.8	13.2
Std Dev	11.4	10.5	14.8	10.8	14.8	10.8
6-7 mos	n = 21	n = 35				
Mean	76.3	82.2	84.7	85.4	15.3	14.6
Median	78	83	83	87	17	13
Std Dev	9.6	10.2	13.4	11.5	13.4	11.5
7-8 mos	n = 40	n = 36				
Mean	77.5	76.4	87.8	80.8	12.2	19.2
Median	78	78	86.7	82	13.3	18
Std Dev	9.6	10.5	14.4	12.2	14.4	12.2
8-9 mos		n = 39				
Mean		80.7		84.5		15.5
Median		83		86.8		13.2
Std Dev		10.8		12.7		12.7

mos = months
 * All Mean, Median, and Std Dev values are shown in percentages
 ** Relative Retained Knowledge and Relative Knowledge Loss are complementary measurements and therefore the means for each treatment group sum to 100%

A different visualization of the relative retained knowledge trend from Table 16 is presented in Figure 5 below, which displays the mean relative retained knowledge percentage referenced to the relative archival score. Archival scores are at 100% because relative to knowledge retention, these scores represent the entirety of knowledge that an individual had previously demonstrated. Neither treatment group drops below 80% relative retained knowledge, with relative loss ranging from approximately 5 - 20% from the archival score for each retention/month group. The ellipses in Figure 5 highlight the groups where significant differences were found.

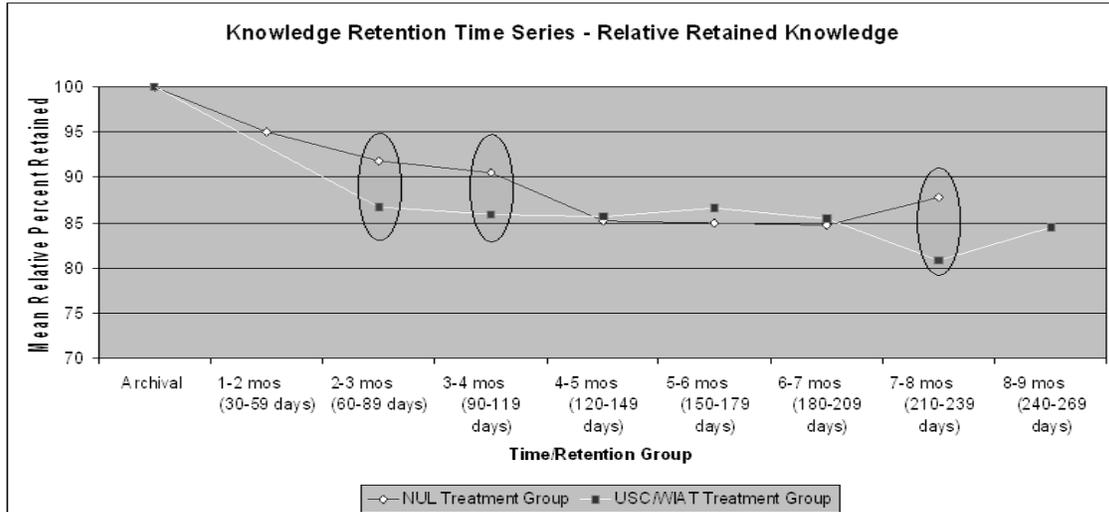


Figure 5. Knowledge Retention Time Series, Relative Retained Knowledge

As previously demonstrated, time (days passed) has a significant negative effect on knowledge retention, as measured by relative retained knowledge. For this reason, an attempt to control for the time distribution between treatment groups was made prior to comparing treatment groups.

The span of NUL treatment retention interval month groups was from 1-2 months to 7-8 months while the USC/WIAT treatment retention interval spanned from 2-3

months to 8-9 months. A traditional ANOVA performed on the days passed between the two treatment groups resulted in a significant difference (F stat = 16.5, pvalue <.0001) with a mean of 129 days passed for the NUL treatment group and 150.5 days passed for the USC/WIAT treatment group. A traditional ANOVA was performed in this case because the days passed variances between treatment groups were found to have no significant difference. In order to minimize the time span differential, the data sets of treatment groups were filtered to include only those retention/month groups that overlapped, which included six group (2-3 months through 7-8 months). This left 485 records, 210 NUL treatment and 275 USC WIAT/Treatment. A traditional ANOVA was again found to be appropriate and performed on the days passed averages between treatment groups. Using a 99% confidence level ($\alpha = 0.01$), it can be stated that there is no significant difference between the average number of days passed (F stat = 4.6, pvalue = 0.03) with an average of 146.5 days passed for the NUL treatment group and 136.2 days passed for the USC/WIAT treatment group. It is appropriate to note that the days passed mean favors the USC/WIAT treatment group (no interactivity) in terms of relative retained knowledge because it has been shown that time does in fact have a significant negative relationship in both treatment groups. Therefore, if any bias exists, it is in the opposite direction of hypothesis 2 which proposed that higher interactivity will result in significantly higher knowledge retention.

In order to ensure that the attempt to control for days passed between the treatment groups and within the month groups was successful, six analysis of variances (ANOVAs) was performed between the six month groups (2-3 months through 7-8 months). Those results are presented below in Table 17.

Table 17. Days Passed between Overlapping Retention/Month Groups for Treatment Group, Welch ANOVA

Retention Interval	F stat	F critical	pvalue
2-3 mos	4.2	6.94	0.04
3-4 mos	0.6	7.33	0.4
4-5 mos	3.9	6.98	0.05
5-6 mos	2.7	7.03	0.1
6-7 mos	2.5	7.28	0.1
7-8 mos	0.8	7.0	0.4

* No significant difference within all month groups is assessed with $\alpha = 0.01$

The next step was to directly test hypothesis 2. As such, independent one-tailed t-tests were conducted for relative retained knowledge between treatment groups and within retention/month groups. The normality assumptions of t-tests were assessed and found to be upheld. When appropriate, the unequal variance t-test method was substituted for a traditional t-test. A 90% confidence level was set for the t-test. It was felt that a lower confidence level was appropriate in that the days passed average favored the USC/WIAT treatment group (no interactivity). The results of the t-tests are shown below in Table 18.

Table 18. Overall Interactivity effect on Knowledge Retention: Relative Retained Knowledge between Treatment Groups and Retention/Month Groups

Retention/Month Group	t stat	pvalue	Significant difference per t-test ($\alpha = 0.1$)
2-3 mos	2.3	0.02	YES
3-4 mos	1.6	0.12	YES
4-5 mos	-0.2 (u)	0.87	NO
5-6 mos	-0.5 (u)	0.59	NO
6-7 mos	-0.2	0.84	NO
7-8 mos	2.3	0.026	YES
2-8 mos (All overlapped intervals)	1.8 (u)	0.07	YES (higher relative retained for NUL treatment)

* (u) Indicates unequal variance t-test was used

Table 16 above demonstrates that for 3 of the 6 month groups, there was a significant difference between the two treatment groups in regards to relative retained

knowledge. In each of the cases of statistical significance, the treatment group that exhibited a higher relative retained knowledge was the NUL treatment group of whom experienced higher interactivity; these findings are in support of hypothesis 2. In the case of considering all overlapping retention interval month groups (2-8 months), the one-tailed Welch t-test showed a significant difference also in support of hypothesis 2 at a 90% confidence level.

H2 and H3: Multiple Variable Effects on Knowledge Retention

The next set of analyses involved the combination effects of the independent variables of time, overall interactivity (H2), and non-CBT instructional exposure (NIE) (H3). A multiple linear regression analysis on the overlapping retention intervals (2-8 months) was deemed appropriate in determining the effects on knowledge retention of these three independent variables. The measure used for NIE in the MLR analysis was the weighted average (NIEWA) as previously described. The distribution of NIE, both weighted and unweighted is shown below in Table 19.

Table 19. Non-CBT Instructional Exposure (NIE) Distribution Characteristics

Sample Group		Weighted Average (NIEWA)	Unweighted Average
NUL Treatment (2-8 months) 210	n =	68.2	45.9
	Mean	49.1	32.6
	Median	74	52.4
	Std Dev		
USC Treatment (2-8 months)	n = 275		
	Mean	50.4	32.2
	Median	27.3	23.9
	Std Dev	57.4	37.7

Based on the skewed distributions of NIE, the median as opposed to the mean provides a better measure of central tendency. The unweighted NIE formula is derived

from the 12 non-medium specific questions dealing with non-CBT exposure frequency that an individual reported to experience on an annual basis. Based upon the unweighted averages, one observes the reporting of exposure to non-CBT IA material approximately 32 days (median) annually for the NUL group and 24 days (median) annually for the USC/WIAT group.

Prior to proceeding with the MLR, an attempt again to control for the days passed average among all independent variables was made. An ANOVA analysis between the mean of days passed for the parameter of NIEWA was conducted. This was to ensure no bias towards groups with lower days passed averages. The result of those analyses and the previous ANOVA between treatment groups for overall interactivity is found below in Table 20.

Table 20. ANOVA, Days Passed within Independent Variable Sets, Both Treatment Groups, Retention Intervals 2-8 months

Independent Variable (Parameter)	F stat	F critical ($\alpha = 0.01$)	pvalue
H2: Overall Interactivity (NUL treatment and USC/WIAT treatment)	4.57	6.75	0.03
H3: Non-CBT Instructional Exposure Weighted Average (NIEWA)	0.01	6.75	0.92

* No significant differences found using $\alpha = 0.01$

Using an α value of 0.01, there are no significant differences found in the mean days passed distributions. Therefore, the MLR analysis on this data set proceeded with relative retained knowledge as the single dependent variable and included the independent variables of time, overall interactivity (H2), and non-CBT instructional exposure weighted average (H3). The techniques of global F-tests, nested linear model comparison, and individual parameter t-tests were used to determine both a parsimonious

and explanatory linear model. The following table displays the statistical calculations found with the inclusion of all three independent parameters:

Table 21. MLR on Time, Overall Interactivity, and Non-CBT Instructional Exposure effects on Knowledge Retention (Both Treatment Groups, Retention Intervals 2-8 months)

Parameter	Parameter Estimates	t-stat	t critical $\alpha = 0.1$	pvalue	Significant parameter per t-test
Intercept	$\beta_0 = 91.1$				
Days Passed (Time)	$\beta_1 = -0.03$	-2.77	-1.284	.006	Yes
Overall Interactivity (Treatment group)	$\beta_2 = 1.28$	2.21	1.284	.028	Yes
Non-CBT instructional exposure (NIEWA)	$\beta_3 = -0.006$	-0.68	1.284	.49	No

The explanatory power of the linear model with all three terms was rather small with an r^2 equal to 0.024. Due to the t-test rejecting the effect of non-CBT instructional exposure on knowledge retention, this term was removed from the developing model. Running the MLR with just the two terms of time and overall interactivity, the linear model exhibited an $r^2 = 0.023$ with both parameter terms passing t-test calculations as derived from their ability to contribute a significant portion to the explanatory power of the model. The parameter estimates were as follows:

Table 22. MLR on Time and Overall Interactivity effects on Knowledge Retention (Both Treatment Groups, Retention Intervals 2-8 months)

Parameter	Parameter Estimates	t-stat	t critical $\alpha = 0.1$	pvalue	Significant parameter per t-test
Intercept	$\beta_0 = 90.7$				
Days Passed (Time)	$\beta_1 = -0.03$	-2.76	-1.284	.006	Yes
Overall Interactivity (Treatment group)	$\beta_2 = 1.23$	2.14	1.284	.033	Yes

Therefore, the first order linear model equation for knowledge retention is shown in Equation 3:

Equation 3. First Order Linear Model Equation, Knowledge Retention

$E(y) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \varepsilon$ <p style="text-align: right; margin-right: 20px;"> <i>y</i> = relative retained knowledge <i>X</i>₁ = days passed (quantitative) <i>X</i>₂ = overall interactivity (qualitative) </p>
--

Since overall interactivity is a qualitative variable that contained two levels (low and none), there are two response functions associated with the final linear model, one function for each overall interactivity category. These two response functions are shown below in Equations 4 and 5.

Equation 4. NUL Treatment Group Response Function, MLR on Time and Overall Interactivity Effects on Knowledge Retention

<p><i>NUL Treatment Group (Low Interactivity)</i></p> $E(y) = (\beta_0 + \beta_2) + \beta_1 X_1$ <p style="text-align: center;">given as</p> $E(\text{relative retained knowledge}) = 91.93 - [(0.03) \cdot (\text{Days Passed})]$ $\text{Mean Confidence Interval} = \pm 1.97\%$

Equation 5. USC/WIAT Treatment Group Response Function, MLR on Time and Overall Interactivity Effects on Knowledge Retention

<p><i>USC/WIAT Treatment Group (No Interactivity)</i></p> $E(y) = (\beta_0 - \beta_2) + \beta_1 X_1$ <p style="text-align: center;">given as</p> $E(\text{relative retained knowledge}) = 89.48 - [(0.03) \cdot (\text{Days Passed})]$ $\text{Mean Confidence Interval} = \pm 1.64\%$

This MLR analysis did not provide support for the effect of non-CBT instructional exposure as measured by NIEWA on knowledge retention but provided further evidence

for the significant effects of time (negative) and overall interactivity (positive) as previously demonstrated by the SLR for time and the t-tests for overall interactivity.

To ensure that the non-significant effect of non-CBT instructional exposure was not specific to just the treatment groups, four MLR analyses were performed on both control and treatment groups using only time and NIEWA as explanatory variables. The results of those analyses are below in table 23. As in all other knowledge retention analyses, an attempt was made to control for time between independent variable groupings. An ANOVA between NIEWA and days passed was performed for all groups below and revealed no significant difference in all groups except the *All groups including control* group. The NUL control group was the only group to demonstrate a significant effect of NIEWA on knowledge retention; the ANOVA for time distribution in this group showed no significant differences at the $\alpha = 0.05$ value (F stat 3.15, pvalue = .08).

Table 23. MLR: Non-CBT Instructional Exposure (NIEWA) effects on Knowledge Retention

Sample Group	r ²	NIEWA t-stat	One-tailed t-critical *	NIEWA pvalue	Significant t per t-test
NUL Control	0.05	1.34	1.29	0.18	YES
NUL Treatment	0.05	-0.71	1.285	0.48	NO
USC/WIAT Control	0.07	-0.93	1.294	0.36	NO
USC/WIAT Treatment	0.01	-0.43	1.284	0.66	NO
<i>ALL groups including control</i>	0.04	0.32	1.283	0.75	NO

* $\alpha = 0.1$

As shown, the only group to exhibit a significant positive effect of NIEWA on knowledge retention, as proposed by hypothesis 3, was the NUL control group. All other groups showed no significant effect per the individual parameter t-tests.

H4 and H6: Job Field and Exploratory Demographic Effects on Knowledge

Retention

The remaining hypotheses in reference to knowledge retention include the effects of job field and the exploratory demographics of major command (*MAJCOM*), *unit*, *employee category*, and attained level of *education*. Analyses for these parameters were conducted independently upon each CBT's aggregated treatment and control groups. Independent analysis of CBT sample groups affords the opportunity to include the entire sample sets, in that the retention interval month groups that did not overlap can be analyzed. Job field was analyzed using a quantitative variable with the two levels of (1) communications or (2) non-communications. The MAJCOM demographic was analyzed only for the NUL, of which contained all nine AF major commands. MAJCOM trends were not analyzed among USC users because users came predominantly from one MAJCOM (88 % Air Force Material Command (AFMC)). In an attempt to search for organization-level trends among USC users, the demographic of *unit* was used with 6 major WPAFB units highly represented. Unit was not used for NUL users because organizational trends were more appropriately searched for in the larger category of MAJCOM. It is important to note that the time-dependent nature of knowledge retention, as supported by previous analyses, causes the need to assess the days passed distributions among the demographic analyses. In order to assess the retention interval differences between demographic categories, multiple ANOVAs were performed. Table 24 records the ANOVA analysis for time and knowledge retention between the remaining qualitative independent variables hypothesized on, in regards to knowledge retention.

**Table 24. Knowledge Retention and Time ANOVAs,
NUL Treatment and Control Group (n = 360)**

Demographic	sample size	Days Passed Mean (Significant Difference per F test with $\alpha = 0.1$)	Relative Retained Knowledge, Mean Percent (Significant Difference per F test with $\alpha = 0.1$)
<u>Job Field</u>			
Communications	129	120.8	90.9
Non-Communications	231	132.8	87.7
		(Yes) p = .08	(Yes) p = .04
<u>Major Command</u>			
ACC	116	126.3	88.9
AETC	36	153.1	88.0
AFMC	24	130.1	89.4
AFRC	11	97.0	91.8
AFSOC	7	150.6	89.8
AFSPC	19	138.6	86.4
AMC	69	132.9	90.2
PACAF	36	93.0	86.0
USAFE	9	146.4	84.1
Other	33	133.8	90.9
		(Yes) p = .004	(No) p = .83
<u>Employee Category</u>			
Enlisted	240	124.6	88.7
Govt Contractor	12	129.8	85.8
Govt Civilian	55	139.2	90.2
Officer	53	135.2	88.7
		(No) p = .35	(No) p = .78
<u>Education</u>			
High School	145	125.4	88.2
Associates Degree	89	133.7	88.6
Bachelors Degree	75	119.0	88.9
Masters Degree	44	145.4	90.1
Doctorate Level Degree	7	124.3	97.5
		(No) p = .19	(No) p = .5

* (Yes) Indicates significant difference per F test
(No) Indicates no significant difference per F test

Significance in knowledge retention was exhibited only for the job field demographic; however the time distribution was also shown to be significant between job fields. Also of note is the significant difference in time for MAJCOM yet no significant difference in knowledge retention.

**Table 25. Knowledge Retention and Time ANOVAs,
USC/WIAT Treatment and Control (n = 384)**

Demographic	sample size	Days Passed Mean (Significant Difference per F test with $\alpha = 0.1$)	Relative Retained Knowledge, Mean Percent (Significant Difference per F test with $\alpha = 0.1$)
<u>Job Field</u>			
Communications	20	169.7	88.3
Non-Communications	364	151.5	84.4
		(Yes) p = .20	(Yes) p = .15
<u>Unit</u>			
445 AW	16	164.4	81.6
74 MDG	34	176.4	78.5
88 ABW	38	153.0	79.8
AFMC	11	162.5	85.5
AFRL	62	109.3	90.1
ASC	120	165.3	85.1
HQ AFMC	40	162.0	86.2
Other	63	146.4	83.7
		(Yes) p < .0001	(Yes) p < .0001
<u>Employee Category</u>			
Enlisted	50	158.9	78.6
Govt Contractor	77	147.1	84.5
Govt Civilian	174	151.2	85.5
Officer	81	154.6	86.3
Other	2	215.5	76.5
		(No) p = .49	(Yes) p = .002
<u>Education</u>			
High School	65	148.0	79.3
Associates Degree	34	153.6	83.4
Bachelors Degree	114	160.3	84.9
Masters Degree	143	153.0	86.8
Doctorate Level Degree	28	126.1	85.3
		(Yes) p = .12	(Yes) p = .0008

* (Yes) indicates significant difference per F test
(No) indicates no significant difference per F test

Significance in knowledge retention was demonstrated for all demographics; however the time distribution was also shown to be significant between all demographics except employee category. Therefore conclusions based on groups with significant time differences should be made with caution.

H5: Job Field and Non-CBT Instructional Exposure

The remaining hypothesis tested was the effect of job field on non-CBT instructional exposure (NIE). Whereas NIE is not a time sensitive variable, it was not necessary to attempt to control for time. However, to ensure there was no time effect on NIE, an SLR analysis was performed and confirmed the time-independent nature of NIE. NIE and overall interactivity are also independent constructs and as such t-tests were conducted upon an aggregate of all four sample groups as well as an aggregate of each CBT sample group (treatment and control). As previously stated, although subjects had the opportunity to report one of several job fields, the data was recoded to include the two categories of (1) communications and (2) non-communications. This was done in order to directly test hypothesis 5a, that subjects who report communications as his/her job field will exhibit a significantly higher non-CBT instructional exposure, as measured by the weighted average measure of NIEWA. The results of t-tests used for hypothesis 5/5a testing are presented below in table 26.

Table 26. Job Field effect on Non-CBT Instructional Exposure

Sample Group	Communications Job Field	Non-Communications Job Field	Significant per t-test
NUL Treatment and Control (n = 360)	n = 129	n = 231	
NIEWA Mean	85.7	65.6	
NIEWA Median	70.9	47.1	YES (u)
Skewness	0.84	1.32	p = .01
USC/WIAT Treatment and Control (n = 365)	n = 20	n = 364	
NIEWA Mean	117.5	44.4	
NIEWA Median	86.6	18.4	YES (u)
Skewness	0.76	1.39	p < .0001
<i>All Sample Groups</i> (n = 744)	n = 149	n = 595	
NIEWA Mean	89.9	52.7	YES (u)
NIEWA Median	70.9	32.6	p < .0001
Skewness	0.92	1.47	

* (u) Indicates unequal variance t-test was used

* Significance at $\alpha = 0.05$ level exhibited in all above analyses

One-tailed unequal variance t-tests revealed a significant difference between NIEWA means at $\alpha = 0.05$ with a significantly higher non-CBT instructional exposure

weighted average for communications job field in all the sample groupings. Although the unequal variances were accounted for, the deviation from normality for NIEWA mean distributions is pointed out. However, all distributions demonstrate a similar right skewness and as previously noted; NWU (2003) state a higher tolerance for non-normal distributions in using t-tests when sample sizes are approximately equal and not too small, as long as a similar skewness is observed. These non-normality exception conditions are met most closely in the NUL treatment and control group but deviations may be too large in the USC/WIAT treatment and control as well as the *all sample groups* analysis. Therefore, for the USC/WIAT group and the aggregate of *all sample groups*, conclusions regarding the effect of job field on non-CBT instructional exposure should be made with caution.

Hypotheses Testing Summary

Table 27 and Figure 6 below summarize the results of the analyses used in testing each hypothesis. When multiple analyses are notated for hypotheses with a sub-hypothesis (H1, H2, H4), each analysis represented a simultaneous testing of both the parent and sub-hypothesis.

Table 27. Hypothesis Testing Results Summary

Hypothesis	Analysis/Analyses	Result
<p>H1: Overall interactivity will positively correlate with learning effectiveness, as measured by initial student performance (initial test score (T1)), therefore...</p> <p>H1a: Because of higher overall interactivity, NUL treatment group users will demonstrate higher levels of learning effectiveness (higher initial test scores (T1)) as compared to USC/WIAT treatment group users</p>	One tailed t-test	Not Supported p<.0001
<p>H2: Overall interactivity will positively correlate with knowledge retention as measured by <i>relative retained knowledge</i>: [(retest score / initial test score) · 100] therefore...</p> <p>H2a: Because of higher overall interactivity, NUL treatment group users will demonstrate higher levels of knowledge retention as measured by relative retained knowledge as compared to USC/WIAT treatment group users</p>	<p>6 Independent t-tests on each overlapping retention interval month groups</p> <p>MLR across all overlapping retention interval month groups</p>	<p>Partially Supported (3 out of 6 groups) pvalue range = .05 - .12</p> <p>Supported p=.033</p>
<p>H3: Non-CBT instructional exposure level will positively correlate with knowledge retention as measured by relative retained knowledge</p>	<p>MLR on treatment groups only across all overlapping retention interval month groups</p> <p>SLR on various sample groupings</p>	<p>Not Supported p=.5</p> <p>Supported in 1 of 4 (NUL Control only) p=.18</p>
<p>H4: Job field will have a significant effect on knowledge retention</p> <p>H4a: Users that report communications as their job field will demonstrate a higher level of knowledge retention as measured by relative retained knowledge as compared to users who report a non-communications job field</p>	<p>ANOVA NUL sample</p> <p>ANOVA USC/WIAT sample</p>	<p>Supported (with caution) p=.04</p> <p>Supported p=.15</p>
<p>H5: Job field will have a significant effect on non-CBT instructional exposure level in that...</p> <p>H5a: Users that report communications as their job field will exhibit a higher non-CBT instructional exposure level than those that report a non-communications job field</p>	<p>t-test on NUL sample</p> <p>t-test on USC/WIAT sample</p> <p>t-test on all sample groups</p>	<p>Supported p=.01</p> <p>Supported (with caution) p<.0001</p> <p>Supported (with caution) p<.0001</p>
<p>H6: Exploratory Demographic effect on knowledge retention</p> <p>MAJCOM Unit Education Employee category</p>	<p>ANOVA on NUL sample ANOVA on USC/WIAT sample ANOVA on NUL sample ANOVA on USC/WIAT sample ANOVA on NUL sample ANOVA on USC/WIAT sample</p>	<p>No significance, p=.83 Significance, p<.0001 No significance, p=.5 Significance, p=.0008 No significance, p=.78 Significance, p=.002</p>

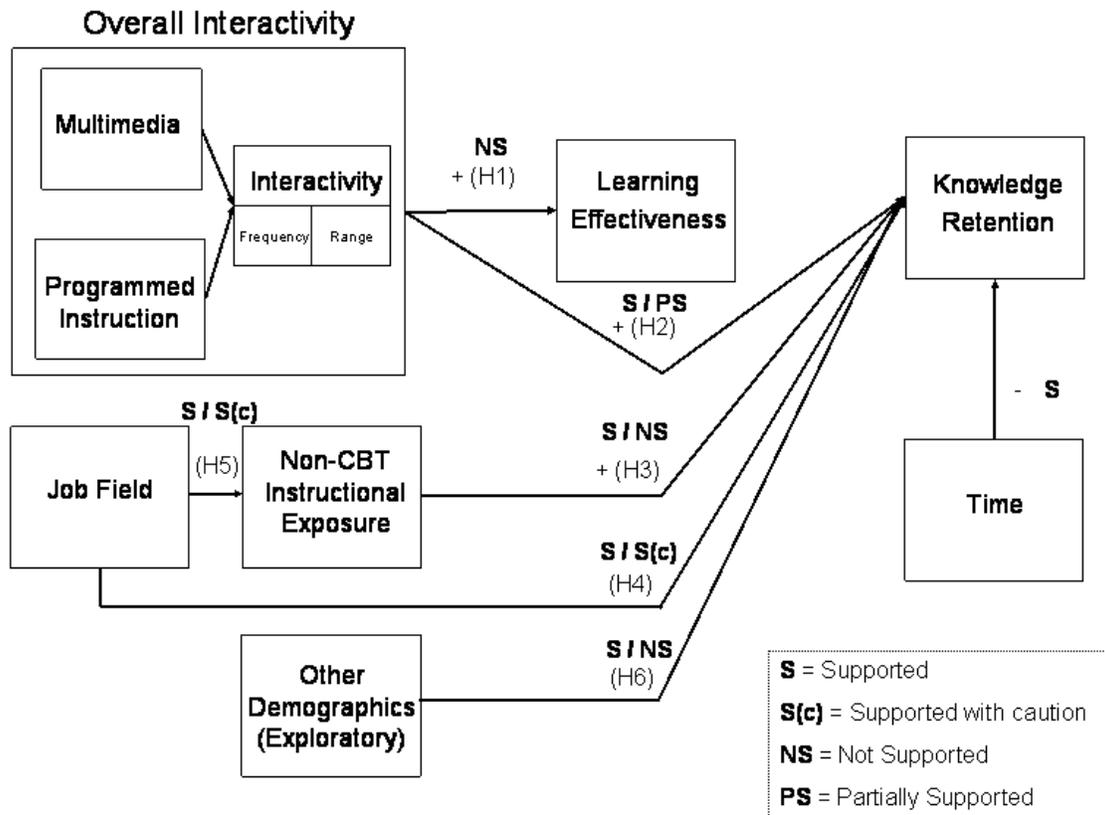


Figure 6. Hypothesis Testing Results, Synthesized Research Model

Figure 6 above shows each case of support for each hypothesis. In cases where more than one statement of support is shown for a hypothesis, this indicates results from either different analyses on the same hypothesis or analyses on different sample groupings for the same hypothesis. Table 27 provides specific sample groups, tests, and results.

Other Analyses

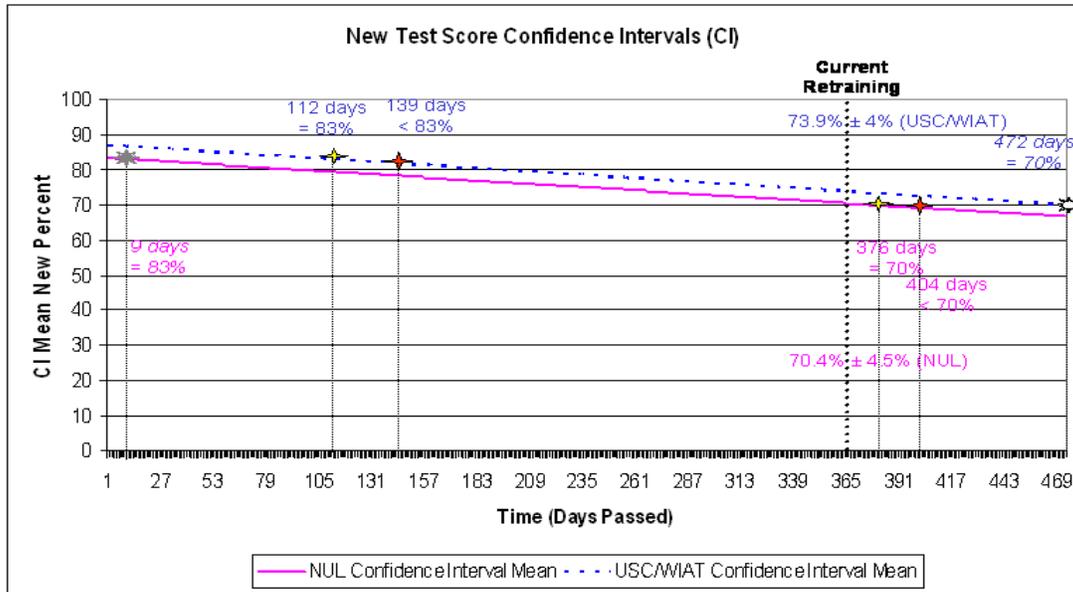
Retraining Intervals for Network End-users, New Test Score Confidence Intervals

Although course knowledge retention among network end-users is a critical measure of sustained learning, USAF Information Assurance managers and leaders are most interested in the time span at which users fall below acceptable passing thresholds and what knowledge level is predominant among users at the current retraining interval of one year. These types of estimates can be made used by employing SLR on the gathered data set of new test scores over time (days passed). In that IA managers and managers also are not necessarily concerned with whether or not users review the CBT courses prior to the taking the tests, analyses were conducted independently on each aggregated CBT treatment and control group (NUL and USC/WIAT). Since the pass/fail thresholds differ for each CBT, analyses were done for each CBT-specific pass/fail threshold. Analyses were also done with respect to the other CBT's pass/fail threshold (NUL users analyzed with USC/WIAT pass/fail threshold and USC/WIAT users analyzed with NUL pass/fail threshold); these analyses were done to determine how users from one sample CBT group would fare with the other groups imposed pass/fail thresholds. The results of the SLR and mean confidence interval calculations for new test score percentage are shown below in both tabular and graphic format in Table 28 and Figure 7.

Table 28. Retraining Interval Assessment: New Test Score Linear Equations and Mean Confidence Intervals

Sample Group	Linear Equation and Confidence Intervals
NUL Treatment and Control n = 360	$E(\text{New Percent}) = 83.32 - (0.0354 \cdot \text{Days Passed})$ $r^2=0.038$
	95% Mean Confidence Interval at 1 year = 70.4% ± 4.5% <i>*estimation is outside the range of sample x values</i>
	95% Mean Confidence Interval = 70% (NUL P/F threshold) at 376 days (11 days beyond 1 year retraining period) and <70% at 404 days (39 days beyond 1 year) <i>* both estimations are outside the range of sample x value</i>
	95% Mean Confidence Interval of 83% (USC/WIAT P/F threshold) at 9 days (356 days before 1 year retraining period)
USC/WIAT Treatment and Control n = 384	$E(\text{New Percent}) = 87.04 - (0.0361 \cdot \text{Days Passed})$ $r^2=0.038$
	95% Mean Confidence Interval at 1 year = 73.9% ± 4% <i>*estimation is outside the range of values of x in sample</i>
	95% Mean Confidence Interval = 83% (USC/WIAT P/F threshold) at 112 days (253 days before 1 year retraining period) and <83% at 139 days (226 days before 1 year retraining period)
	95% Mean Confidence Interval = 70% (NUL P/F threshold) at 472 days (107 days beyond 1 year) <i>*estimation is outside the range of sample x values</i>

*P/F: Pass/Fail



- CI Mean = CBT-specific pass/fail threshold
- USC/WIAT CI Mean = NUL pass/fail threshold
- CI Mean < CBT-specific pass/fail threshold
- NUL CI Mean = USC/WIAT pass/fail threshold

Retention Interval samples for NUL ranged from 32-239 days, for USC/WIAT ranged from 65-265 days

Figure 7. Retraining Interval Visualization: New Test Score Confidence Intervals

New Percent Score between NUL and USC/WIAT Treatment Groups

Although it was shown that the NUL treatment group, which experienced higher overall interactivity exhibited higher levels of relative retained knowledge, it is also evident that the raw level of knowledge, as measured by new test score percent, was much higher in the USC treatment group. This caused a desire to determine if this difference was statistically significant. Therefore, a t-test of new test scores between treatment groups was performed across overlapping retention intervals (2-8 months). It was found that the USC/WIAT treatment group exhibited a significantly higher new test score (t stat = 4.948, pvalue <0.001). It is also worth noting that the USC/WIAT treatment group also had a significantly higher archival test score.

Control and Treatment Groups

In order to assess the differences in relative retained knowledge and new test scores between treatment and control groups, four t-tests were performed within each CBT user sample set.

The results for *relative retained knowledge* were: no significant difference in relative retained knowledge between the NUL treatment and control groups (n = 360, t stat = .034, pvalue = 0.97), but a significant difference was found between means for relative retained knowledge of the USC/WIAT treatment and control groups (n = 384, t stat 2.697, pvalue.007) with a significantly higher mean relative retained knowledge in the USC/WIAT treatment group. It is noted that although the mean for days passed between the USC/WIAT treatment and control groups were not significant ($\alpha = 0.01$) (the same α level used for all time control attempts), the treatment group did have a lower average number of days passed (by 11 days).

The results for *new test score* were: no significant difference in the mean new test score between the NUL treatment and control groups (t stat = 0.33, pvalue = 0.74), but a significant difference was found between the mean new test score of the USC/WIAT treatment and control groups (unequal variance t stat = 2.62, pvalue = 0.01).

Non-CBT Instructional Exposure (NIE) Descriptive Statistics

Although the weighted average of non-CBT instructional exposure (NIEWA) was used in analyzing NIE as an independent variable affecting knowledge retention, a description of the ordinal data reported by each CBTs user population is central to answering one of the research questions originally proposed. That research questions asked: how robust and diverse are USAF IA training and awareness programs? An analysis of the ordinal responses within the NIE survey is felt most appropriate in answering this research question. Analysis was performed on independently on both aggregated treatment and control CBT sample groups. Such an assessment can serve a baseline NIE measurement of which to compare future assessments. Tables 29 and 30 below display the proportion of users that reported each of the exposure frequencies for the 12 medium-specific Information Assurance (IA) NIE survey questions and the 1 non-medium-specific question. In some cases, where three or less individuals reported a particular frequency, and from rounding to the second significant digit, the check sum is slightly off. The specific questions asked for each medium can be found in Appendices D and E, questions a through m.

Table 29. NUL Users (Treatment and Control): Non-CBT Information Assurance Instructional Exposure Frequency Reporting, Proportion Statistics

<i>n</i> = 360	never	annually	bi-annually	quarterly	monthly	weekly	daily
Posters	.19	.13	.09	.13	.16	.12	.18
Videos	.33	.33	.15	.13	.05	.01	.003
Newsletters	.17	.06	.06	.18	.25	.19	.09
Articles	.17	.06	.04	.20	.25	.19	.09
Emails	.07	.04	.02	.18	.28	.29	.12
Military websites	.19	.11	.08	.16	.20	.16	.10
Non-military websites	.06	.94	0	0	0	0	0
Lectures	.54	.25	.09	.10	.02	.003	0
Workshops	.69	.17	.07	.06	.01	.003	0
Computer software	.32	.13	.06	.07	.05	.06	.31
Hands on practice	.32	.08	.04	.06	.05	.08	.37
Senior leaders	.11	.16	.10	.23	.20	.11	.09
<i>All mediums</i>	.05	.05	.05	.12	.14	.16	.43

Table 30. USC/WIAT Users (Treatment and Control): Non-CBT Information Assurance Instructional Exposure Frequency Reporting, Proportion Statistics

<i>n</i> = 384	never	annually	bi-annually	quarterly	monthly	weekly	daily
Posters	.25	.10	.10	.19	.13	.12	.11
Videos	.49	.22	.11	.15	.02	.01	.003
Newsletters	.18	.05	.07	.28	.24	.15	.03
Articles	.20	.05	.07	.24	.25	.15	.04
Emails	.08	.04	.04	.22	.33	.23	.06
Military websites	.35	.10	.12	.20	.10	.08	.05
Non-military websites	.09	.91	0	0	0	0	0
Lectures	.51	.21	.13	.15	.008	0	0
Workshops	.76	.14	.04	.05	.01	.003	0
Computer software	.46	.10	.06	.06	.06	.05	.21
Hands on practice	.45	.10	.03	.06	.05	.03	.28
Senior leaders	.16	.13	.12	.31	.18	.08	.02
<i>All mediums</i>	.06	.07	.04	.17	.19	.20	.27

A visual assessment of these tables 29 and 30 identifies that there is some evidence of both robustness and diversity within the Information Assurance training and awareness programs both AF-wide and local to WPAFB. Coupling these analyses with the NIE unweighted averages in Table 19 leads to an evaluation that at least for the treatment groups, the NUL sample appears to experience a slightly more robust (more frequency) as compared to the USC/WIAT treatment group (NUL NIE unweighted median = 32.6 days, USC/WIAT NIE unweighted median = 23.9 days). Overall, these findings demonstrate a significant effort by base-level IA managers to convey critical information regarding network and information security issues through a variety of different means, thus increasing the potential for gains in awareness and training levels across the user population.

Summary

This chapter discussed the implementation of the research design including the content analysis, quasi-experimental, and survey portions. The measurements and formulas used for each construct of interest were specified as well as coding techniques where appropriate. The analyses results specific to all proposed hypotheses were presented in narrative, table, and figure formats. Also included were analyses not specific to hypotheses but rather deemed useful for practitioner/managerial use, this research endeavor, and/or future research. The next and subsequently last chapter will provide a discussion of the findings, their limitations, as well as practical and academic implications.

V. Discussion and Conclusions

Introduction

This final chapter will discuss the findings of the analyses in Chapter IV and the derived conclusions in answering the proposed research hypotheses and research questions. The limitations of this research endeavor are noted. Implications for academics and future research are outlined. Practitioner-focused implications on the future of network security training programs will also be discussed.

Limitations

Although this study assessed a diverse group of U.S. Air Force users, including individuals from all employee categories and across all major commands, it explored construct relationships in just two U.S. Air Force CBT courses among the many thousands in existence. For this reason, the generalizability of the results do not necessarily apply to other CBTs or to populations outside the U.S. Air Force.

The time-sensitive nature of knowledge retention and the large range of retention intervals studied made it difficult to compare sample groups with exact retention interval distributions. Attempts were made to control the time variable by using high confidence coefficients in assessing differences in retention interval distributions among sample groupings. Utilizing lower confidence coefficients would have resulted in different conclusions regarding the retention interval differences between groups.

A critical piece in studying learning outcomes over time is an evaluation of knowledge levels prior to initial training. This study was unable to measure this part of the time series and therefore could not provide a baseline level of knowledge prior to

course treatment. Without such evidence, conclusions about course effect on learning are limited.

Course exams strive to measure actual student knowledge levels. However, the subject matter, as well as the exam questions within the two CBT courses that were studied, has been present in the USAF for a number of years. This realization of potential test-retest invalidity may affect the ability of the exams to assess actual knowledge levels at any given time period because issues of learning the test, learning the answers, and improved test-taking ability may interfere with any attempted measurement of knowledge level. Also as mentioned in Chapter II sections on the NUL and USC/WIAT, there is evidence that the databases store only the last test score obtained by an individual. This action causes suspicion into the validity of reported scores.

A limited level of explanatory power for knowledge retention was found in this study. This is noted as a limitation in making conclusions about factors affecting this key learning outcome construct. Knowledge retention values at all time periods were found to occur across a wide range of values. This variance had an effect on the explanatory power of the models. It is clear that there are other factors significantly affecting the construct of knowledge retention.

Discussion of Hypotheses Findings

The three primary hypotheses were: associating the construct of overall interactivity to learning effectiveness (H1) and knowledge retention (H2) as well as associating the construct of non-CBT instructional exposure (NIE) with knowledge retention (H3). As chapter IV outlined, there was a mix of results pertaining to the

proposed hypotheses; some as expected, some not as expected, and some not significant. In reference to the effect of interactivity on learning effectiveness, the data did not support the hypothesis that overall interactivity would positively correlate with learning effectiveness. In fact, higher learning effectiveness was found in the no interactivity group. As hypothesized, there was support that overall interactivity within CBTs positively affects knowledge retention. This finding is congruent with the literature and reinforces the link between engaging learning environments and positive learning outcomes. The hypothesis that non-CBT instructional exposure, particularly of an IA nature, would have a positive effect on knowledge retention also received partial support.

Learning Effectiveness

The finding of lower learning effectiveness in the higher interactivity group is counter to the literature on the subject of interactivity. Although the primary design difference between the two CBTs was interactivity levels, a main implementation distinction was a large difference in the course exam pass/fail thresholds. This difference in pass/fail thresholds may have had a significant and overshadowing effect on learning effectiveness. The two CBTs studied had interactivity and pass/fail thresholds on opposite ends; the NUL CBT contained higher interactivity but implemented a lower pass/fail threshold (70 %, 13% lower), while the USC/WIAT CBT contained lower interactivity (none) but implemented a higher pass/fail threshold (83%, 13% higher). The constructs of learning effectiveness and knowledge retention are explicitly related. The finding of lower interactivity and higher learning effectiveness, combined with the finding of lower interactivity and lower knowledge retention, can cause suspicion as to the validity of the initial learning effectiveness measurements.

As mentioned, each course's implementation allows users to take the course exams multiple times with no limit on the number of times within any given time period. In that all network end-users must pass this training and a user's last score can be shown to provide adequate proof of training, users may take the test until they receive a passing grade. Such occurrences would inflate the initial learning scores and hence alter the validity of using these scores as a true measure of learning effectiveness.

The initial test score inflation suspicion may also be supported by exact losses in raw knowledge ($T1 - T2$) in the NUL treatment and control groups (10.5%) (Table 11). A follow-up email was sent to the NUL and USC/WIAT control groups to ascertain whether or not this multiple-test/short-timeframe taking strategy is prevalent. One user confirmed the used of this multiple-test/short-timeframe strategy and responded with,

“I did not prepare/review the NUL, but rather went straight to the examination portion, as I'm sure many folks do. I realize this training is important but so is all the other training that has taken this format. I will probably use the same strategy in the future unless the software is changed to prevent it.”

This user's response, coupled with other similar remarks, make the initial learning scores suspect as measures of true learning effectiveness and true knowledge levels.

Knowledge Retention

Knowledge retention was the central learning outcome construct in this study. Of primary interest were the effects of overall interactivity and non-CBT instructional exposure on knowledge retention. Also of interest were the effects of job field and other demographics on knowledge retention. As noted, there was significant support for the positive effect of overall interactivity on knowledge retention. This finding is congruent with the reviewed literature and reinforces the well-documented link between social and engaging learning environments with positive learning outcomes (Jung et al., 2002;

Muirhead, 2000; Oliver et al., 1996; Vygotsky, 1978). The nature of knowledge loss as exhibiting a steep initial drop followed by an asymptotic leveling over time was also found to be upheld in this study.

The hypothesis that Information Assurance non-CBT instructional exposure (IA NIE) would have a positive effect on knowledge retention also received partial support by showing a significant effect in the NUL control group. The construct of IA NIE attempted to capture the levels at which users were exposed to learning activities related to the concepts within each CBT course. Although only supported in one of the four treatment groups, this finding provides some evidence of the documented link between higher knowledge retention and learning activities related to course content (Wisher et al., 2001). It is believed that the link was not found to be stronger because the NIE questions inquired about exposure to information and network security issues/concepts in general and were not specific to the questions contained on the CBT course exams. However, the CBT courses studied do not include all pertinent network end-user knowledge. Therefore the use of multiple mediums for the transfer and acquisition of information and network security knowledge beyond the CBT content is deemed a worthwhile effort.

The analysis of job field impact and other demographics on knowledge retention resulted in mixed outcomes. Demographics explored included: employee category, education, major command (MAJCOM) for the NUL sample group, and unit for the USC/WIAT group. Employee category included the groups of enlisted, officer, government civilian, and government contractor. Education was recorded as one of five

attained levels: high school, associate's degree, bachelor's degree, master's degree, and doctorate level degree.

There were no significant differences found among employee categories or education levels in the NUL sample; however, within the USC/WIAT sample, both demographics showed significant differences in that the categories of enlisted and high school tended to exhibit lower knowledge retention. Some studies have addressed the relationship between a lack of computer education/experience with lower learning outcomes in CBT environments (Williams and Zahed, 1996). This link may explain the finding of lower knowledge retention in the two categories of enlisted and high school.

There were no significant differences found among MAJCOMs for knowledge retention in the NUL sample group - even though the retention intervals were significantly different. Interestingly, PACAF had the lowest mean retention interval (93 days), which would be expected to correlate with one of the higher levels of knowledge retention. In fact, PACAF had the 2nd lowest level of knowledge retention. AFRC had the second lowest mean retention interval (97 days) and although it did exhibit the highest knowledge retention interval, it was not significant enough to be deemed statistically higher than the other groups. These findings are useful in extracting organizational trends.

Job Field, Knowledge Retention and Non-CBT Instructional Exposure

It was hypothesized that users in a communications job field, when compared to those not in a communications job field, would exhibit both higher levels of non-CBT instructional exposure (NIE) and knowledge retention. There was evidence for both of these proposed relationships. The logic behind job field effect on NIE is that users in the

communications field are more likely to experience information and network security issues outside the training CBTs. The logic behind job field's direct effect on knowledge retention is rooted in its relationship with NIE. The results from the study confirm the logic of these hypotheses as extending into actual practice.

Implications for Academia and Future Research

This study involved the comparison of one CBT with no interactivity and one with low interactivity. CBTs exist that employ a much higher level of interactivity than present between the two courses studied (*None* and *Low*). In that interactivity was shown to have a significant positive effect on knowledge retention, future studies may search for learning outcome differences among a wider range of interactive CBTs to include those courses evaluated as having medium and high interactivity.

Statements from several users indicated the presence of stale and extremely familiar course content. It is important not only to assess whether or not training material is effective, but whether or not it is relevant and current as well. An in depth study into whether or not the course content is current and relevant for today's network security environment and end-user experiences would prove to be a worthwhile research effort.

This study also uncovered a potential link between pass/fail threshold and learning effectiveness. Goal-setting theory literature supports the use of imposing challenging but attainable goals in promoting increased effectiveness and motivation (Latham and Locke, 1984). Theories on goal-setting could uncover the root cause of this finding. Future studies could more explicitly test the suspected relationship between pass/fail threshold and initial learning.

This study provides a significant contribution for academia and future research in that it provides a methodology framework and research model which can be utilized for future learning outcome assessments of computer-based training courses.

Implications and Recommendations for Practitioners

This study has several implications for Information Assurance practitioners, ranging from unit-level and base-level Information Assurance professionals, up to the highest echelon of Air Force communications and information leaders. Findings should help to shape future versions of CBT design and implementation, as well as network end-user training policy and management. Recommendations include:

(1) Many users reported that current network security CBT material is very familiar.

Recommend an immediate update/refresh of the content within the network security training courses.

(2) This study provided evidence that interactivity can enhance knowledge retention. In that the highest level of CBT interactivity was assessed as *LOW*.

Recommend adding more interactivity to the network user training courses in hopes of further improving knowledge retention. Possible enhancements to interactivity include:

- a. Adding multimedia content such as *value-added*: graphics, animations, voice, and video.
- b. Increased opportunities for meaningful learner input and participation beyond multiple-choice questions. For instance, multi-level simulations of probable end-user network security events (suspicious emails, virus infections, etc.) could be presented. Users would then be prompted to react and make

informed decisions of which would affect the next stage of the simulation (Barron, 1998).

- c. The addition of adaptable training features capable of individualizing the presentation of course material based upon assessed levels of baseline knowledge, preferred delivery mode, and mastery of new material (Oliver et al., 1996; Wonacott, 2000). Such a design allows for the opportunity of scaffolding.
- (3) The addition of supplemental/optional course material of a more in-depth nature. Several users in the study stated that they skipped right to the test because they feel confident in knowing the test material. This is beneficial in not forcing users to review well-known material, however providing more advanced content for these more experienced users provides the opportunity to further enhance the knowledge base of the end-user population.
 - (4) There was some evidence that users take advantage of the lack of course exam proctoring by utilizing a multiple-test/short-timeframe strategy. The development of learning management system features that can detect, discourage, minimize, and/or prevent such activity is recommended.
 - (5) AFCA IA management indicated a widespread use of CD and download versions of the NUL course, especially for new base network users. AFCA management also conveyed that although users have the ability to upload their results to the AFCA database following completion of either the CD or download version, many results are not uploaded. The widespread use of the CD version was believed to occur because of the security requirement to not allow users on a base network until passing

the NUL course. However, this situation restricts AFCAs ability to centrally manage the training of network end-users by both limiting its view of user scores and its ability to ensure users receive the most current version of training. It is recommended that a security work-around for CD versions be implemented at AF bases. A workaround could include the configuration of a “locked-down” PC with access only to the AFCA NUL training website. It is also recommended to highly encourage that all course completions that take place “offline” have their scores uploaded to AFCA. These recommendations are made in order to increase the likelihood that all user training records are forwarded to AFCA. This would increase the management and research capability of AFCA by providing a larger view of actual NUL user data.

- (6) Strive to maintain and increase the robustness and diversity of the USAF Information Assurance Education Training and Awareness programs as identified in Table 29.
- (7) This study found evidence for links between higher pass/fail thresholds and increased learning effectiveness, as well as increased interactivity and knowledge retention. Implementing a combination of increased CBT interactivity and a higher pass/fail threshold could result in both higher initial learning (learning effectiveness) and increased knowledge retention.

This study also analyzed user knowledge levels over time in relation to pass/fail thresholds and the current retraining timeline of one year (see Table 28 and Figure 7). The NUL CBT implements a pass/fail threshold of $\geq 70\%$, while the USC/WIAT implements a threshold of $\geq 83\%$.

The average new test score for an NUL user is predicted as 70.4% at the one year timeframe, 70% at the 376 day timeframe, and <70% at the 404 day timeframe.

Therefore, with the current NUL threshold of 70% in place, it appears that the current retraining timeline is appropriate in that the average user score continues to be above the threshold beyond the mandate of retraining.

The average new test score for a USC/WIAT user is predicted as 73.9% at the one year timeframe, 83% at the 112 day timeframe, and <83% at the 139 day timeframe.

Therefore, with the current USC/WIAT threshold of 83%, a one-year retraining timeline does not seem adequate in that the average new test score is predicted to drop below the threshold 7 ½ months before retraining. One strategy in preventing the average score from dropping below the current threshold includes shifting the retraining timeline from annually to every 4 ½ months. Others could include the implementation of a more interactive training program with higher knowledge retention rates.

Another issue to address is the existence of a pass/fail threshold difference. It is not clear why WPAFB users are held to a higher standard of content knowledge than its NUL counterparts. It would not be advisable for WPAFB IA personnel lower their standards but perhaps the AFCA IA personnel should raise their standard. This issue of uneven standards is something that IA practitioners need to address and remedy.

Conclusion

There is no doubt that it is fiscally unfeasible to traditionally train all network end-users. The use of computer-based training creates a great potential for fiscal savings, time efficiency, and learning gains. However, learning gains will not be realized unless the true aim of training, that is increasing and sustaining knowledge and skill levels,

remains the focus of training programs and future CBT development. By mandating network security training for all end-users (a population which exceeds one-million individuals) the USAF acknowledges the importance of this training arena. As with all teaching and training endeavors: the delivery mode, course content, and learning outcomes must be evaluated on an ongoing basis. The CIO-published Federal Information Security Assessment Framework (FISAF) recognizes the need to not only train employees on security requirements but to “plan, implement, maintain, and evaluate an effective training and awareness program” (FISAF, 2000). However, the absence of studies on CBT effectiveness, make apparent a lack of maintenance and evaluation activities associated with end-user network security training. Neglecting the key stages of maintenance and evaluation in the training life-cycle will no doubt prove detrimental to this program’s effectiveness for learning outcomes such as effectiveness and retention.

CBTs will most likely dominate the USAF training environment of the future; therefore there is a clear need for more formal and longitudinal learning outcome research within this training domain of AF CBTs. Learning outcomes cannot be assumed for any instructional method and CBTs are no different. A lack of formal evaluation can only lead to uninformed decisions and unfounded beliefs about the state of our network security. Such decisions do not contribute to our pursuit of information superiority and most importantly degrade our decision superiority.

Network end-user training must remain current with changing technologies and evolving threats. There is evidence that the current training content is in fact stale and possibly even outdated. The landscape of annual training requirements for USAF personnel is becoming continually more crowded (Privacy Act, Law of Armed Conflict,

Self Aid Buddy Care, Anti-Terrorism, etc.). If the aim of the network user licensing mandate is to promote awareness, increase knowledge, and improve skills in the arena of information and network security, then the training content must remain fresh, current, and engaging, as well as relevant for user experiences. These training content characteristics should be prevalent in all training programs. Current research in the area of technology-assisted learning may aid in providing the much needed dynamic CBT content.

The U.S. government, through its Advanced Distributed Learning (ADL) initiative, is currently researching and testing new learning technologies that provide truly adaptive content and testing, as well as interactive human-computer exchanges (Fletcher, 2002). The ADL initiative is led by the Department of Defense in coordination with other federal agencies. Applying emerging ADL technologies to critical training arenas, such as network security, can help provide a current and engaging learning environment by individualizing course content. The hopes in creating an adaptable computer learning environment more conducive to expanding individual knowledge is that by doing so, personnel will show gains in both learning effectiveness and knowledge retention. These gains in learning and retention for network security training can help fortify the defense of information/network assets by improving the most critical piece of the USAF multilevel information security architecture — our people.

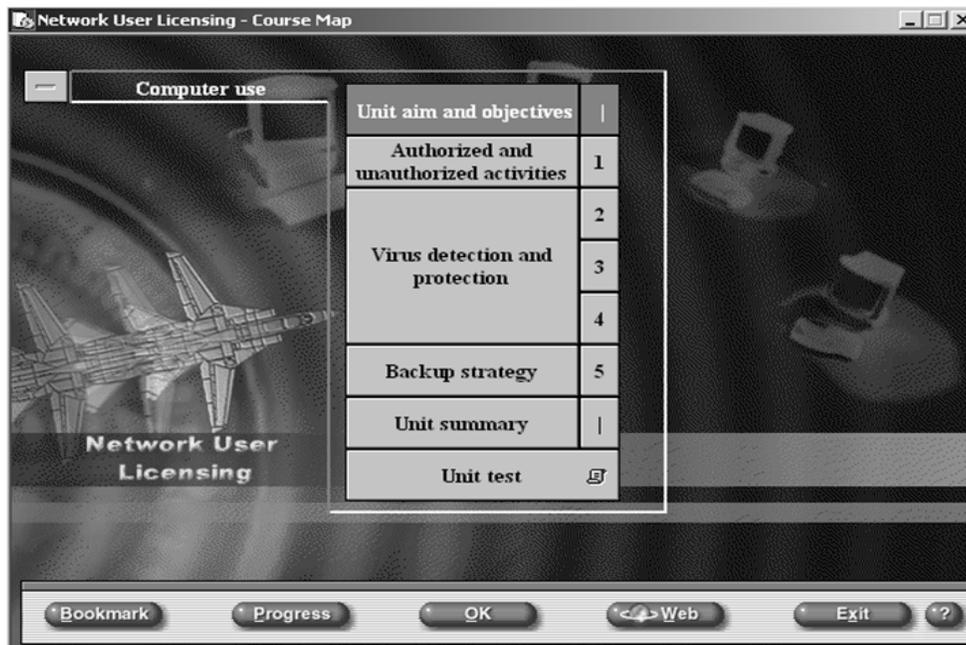
Appendix A: AFCA NUL CBT screenshots with narrative

NUL Course Information Page

Course Information Page	
Name:	Network User Licensing
Code:	YAF06SE
Language:	English
Status:	RELEASED
Audience Details	
Duration (hrs):	1
Prerequisites:	None
Audience:	All USAF and civilian personnel who use computers on USAF networks
Aim:	This course introduces the student to the rules and regulations governing the use of computers on USAF networks
Learning Objectives:	After taking this course, the student should be able to: <ul style="list-style-type: none"> differentiate between authorized and unauthorized information system use
Structure:	1. Computer use <ul style="list-style-type: none"> - Authorized and unauthorized activities - Virus detection and protection - Backup strategy
Learning Path Info:	Customisation for USAF

Opening course frame

Note the sections and navigation links at the bottom of the frame.



Computer Use Section of course

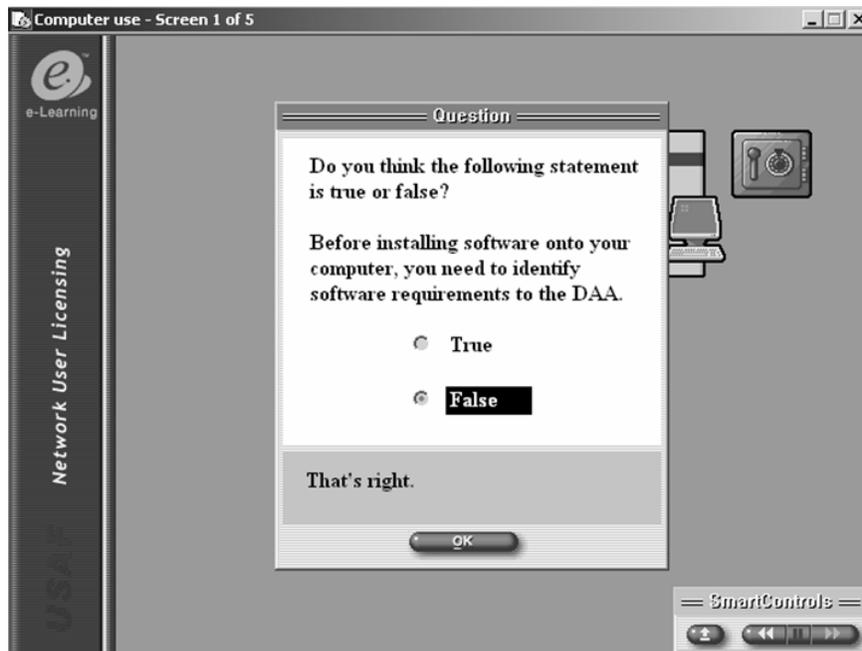
Below is an embedded section question. This represents the implementation of both a programmed instructional approach and user input/interaction opportunities. Throughout the entire course, the NUL has 9 embedded section questions. The *SmartControl* icons at bottom right of frame provide users the ability to navigate through the course.



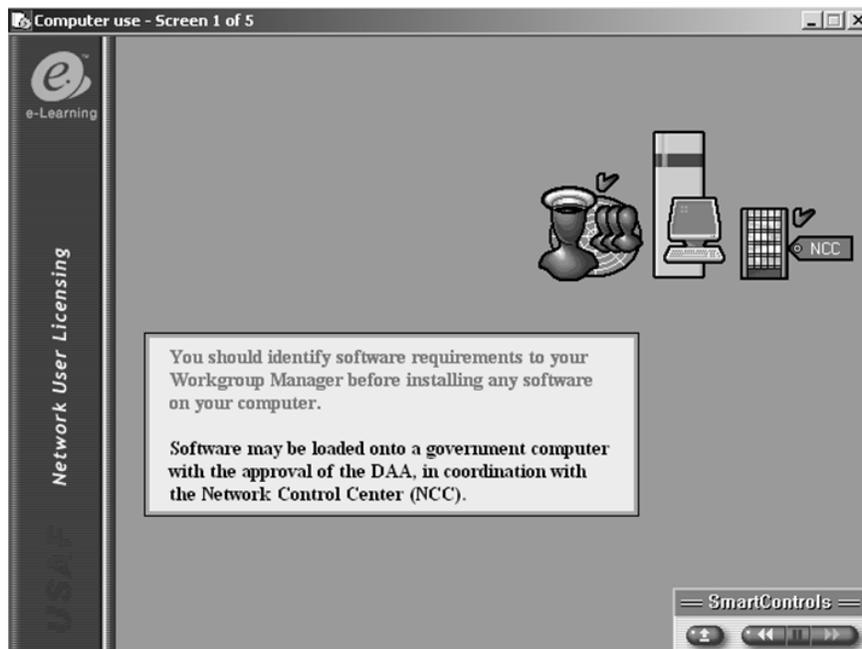
Below is the result of entering a wrong answer. In certain embedded questions, when the wrong answer is entered, the CBT informs a user that his response is incorrect and restates the correct answer.



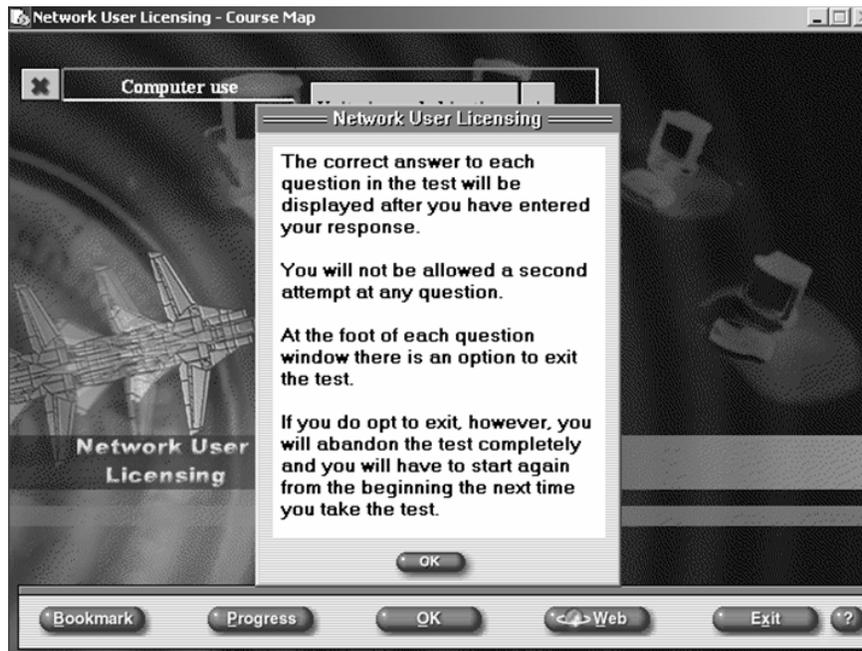
Below is the result of entering a right answer. As shown, confirmation of the right answer is provided.



As shown below, "normal" course content resumes following each embedded question.



NUL End-of-Course Test/Exam, Exam Introduction



NUL typically contains 23 end-of-course test questions (same as USC//WIAT). For questions 1-7 and 9-23, NUL test questions and answers are *identical* in all respects to the USC/WIAT end-of-course test.

NUL question 8 is different in all respects from USC/WIAT question 8 (different question and different answers). The topic of question 8 is altogether different. NUL's question 8 inquires about the nature of a virus while USC/WIAT's question 8 inquires about releasing personal network passwords.

NUL keeps order of questions constant for individuals that take the end-of-course test directly following completion of the of the course; otherwise, users who skip right the end-of-course exam receive a randomized 13 question set from the 23 item question pool; however, answer order remains the same.

Other test differences, both major and minor are shown below in the table.

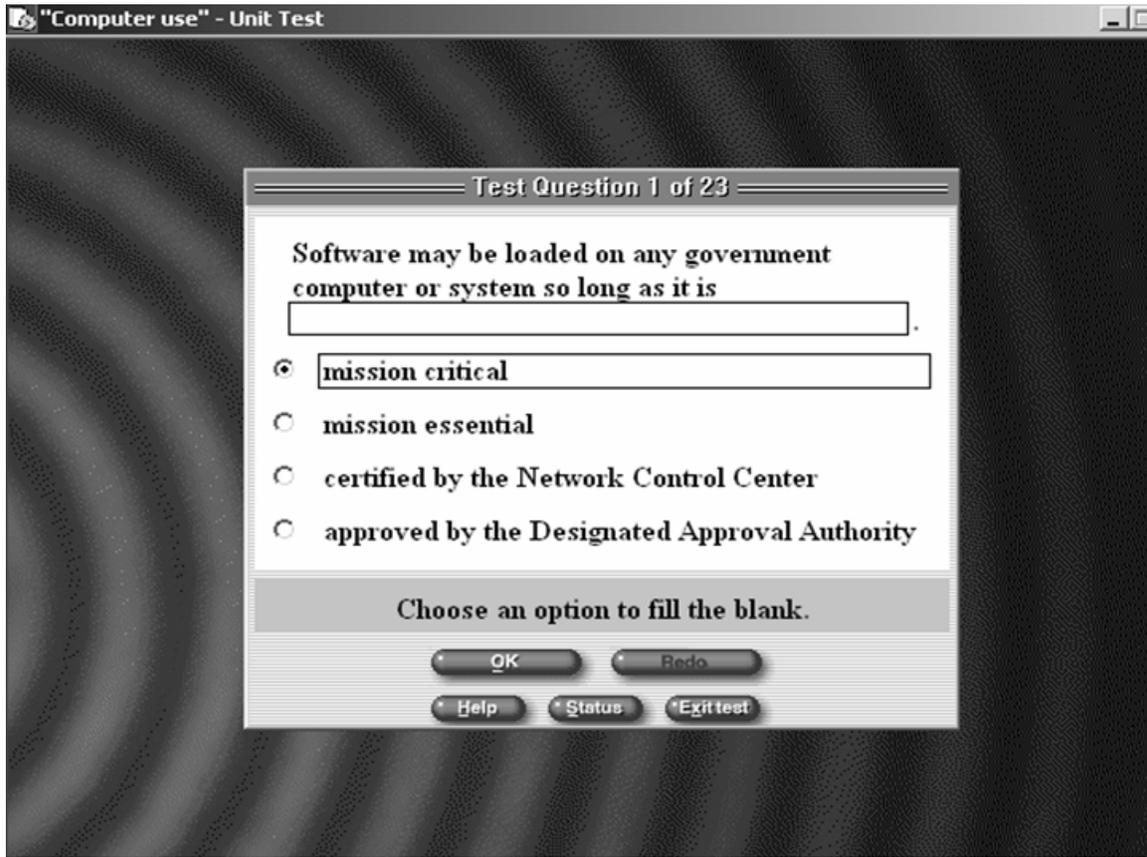
NUL and USC/WIAT End-of-Course Test Differences

MAJOR	MINOR
(1) Pass/Fail Threshold: NUL's pass/fail threshold is $\geq 70\%$ (≥ 16 out of 23) correct; USC/WIAT's pass/fail threshold is $\geq 83\%$ (≥ 19 out of 23) correct	(1) NUL presents questions on individual pages, while USC/WIAT presents all questions on the same webpage
	(2) NUL provides the correct answer and a following each question and a test summary while USC/WIAT provides only a summary of the number correct after answering <i>all</i> questions <ul style="list-style-type: none"> a. NUL sometimes expands upon the correct answer following a question; USC/WIAT does not. b. NUL presents the answers and radio buttons to force one answer response. USC/WIAT does the same but includes a letter designation before each answer choice (a, b, c, d); NUL has no letter designation for each answer choice.
	(3) If individuals choose to skip to the end-of-course test, (without first reviewing the course) NUL presents only 13 questions from the bank of 23 questions; USC/WIAT always presents all 23 questions.

As noted throughout this research, the primary design difference between NUL and USC/WIAT is differing levels of interactivity; NUL was assessed as having *Low* interactivity and USC/WIAT as *No* interactivity.

The primary course content difference between NUL and USC/WIAT is an additional course section titled *Computer Security Controls* in USC/WIAT (Appendix B). The *Computer Security Controls* section in USC/WIAT contains content areas of *user responsibilities* and *password policies*. Some of the information covered in the *Computer Security Controls* section of USC/WIAT is also contained in sections of the NUL CBT.

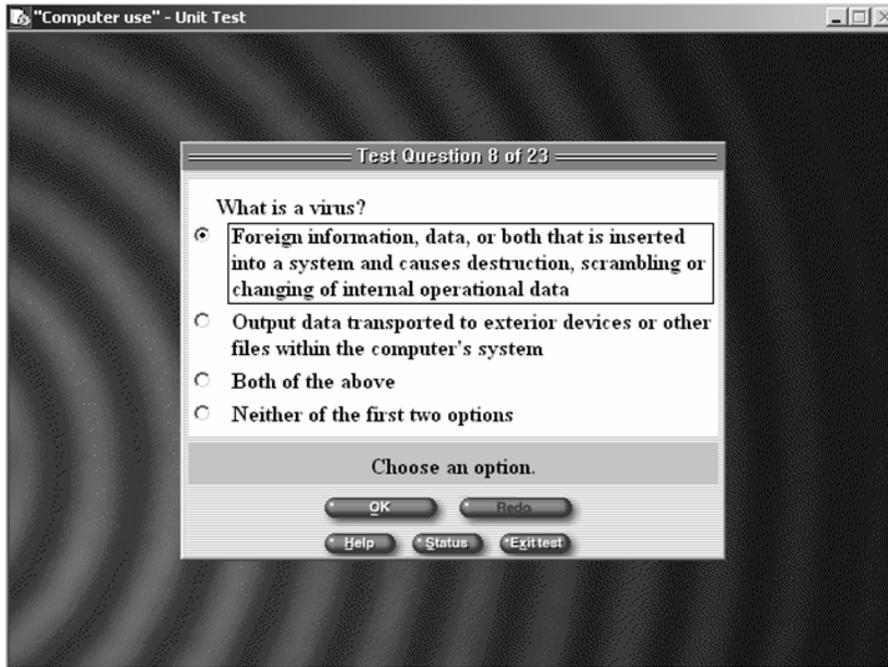
NUL End-of-Course Test Question 1



Although some embedded questions have correct answers which require multiple answer selections, all end-of-course exam questions allow only one answer choice (all of the above, or both of the above, none of the above maybe this one answer choice)

Also, clicking on the *Help* icon contained on all questions describes the nature of the end-of-course exam and how to navigate through the exam and answer questions. *Help* does not provide any answer hints.

*NUL End-of-Course Test Question 8
(The only different end-of-course test question between NUL and USC/WIAT)*



USC/WIAT End-of-Course Test Question 8

8. When is it ok to give out your password?

- a. When your System Administrator or Work Group Manager needs access to your computer.
 - b. Give to a co-worker while you are on vacation.
 - c. Never, no one should ever ask you for your password.
 - d. Both A and B are correct.
-

Appendix B: WPAFB User Sate CBT (USC)
Available at <https://www.asc.wpafb.af.mil/base/c4/iaap/usertraining.htm>



**USER
SATE
CBT**



This Test is for Wright-Patterson AFB Personnel only
Below is the authorized "Local Initial and Refresher SATE Training"

If you are a System Administrator or Work Group Manager, and have taken the "Information System User", 4.5 hour CBT on the Denver site during the 2001 calendar year, you do not have to take this "Local Initial and Refresher SATE Training".
However you do have to provide proof of training to your unit SATE manager.

Mark **"Initial Training"** if you have just received access to your information system account. You have a maximum of 60 days to complete this training. Your unit may require you to complete the training in less than 60 days.

Mark **"Refresher Training"** if you are taking this training to fulfill the annual SATE training requirement. Refresher Training is required annually.

- [Course Text](#) for "Local Initial and Refresher SATE Training"
- [Course Exam](#) for "Local Initial and Refresher SATE Training"

SATE User Training Information

The following represents the actual online course available at <https://www.asc.wpafb.af.mil/base/c4/iaap/train/train-docs/usertext.doc>. It is comprised only of the following text.

Computer Use

Authorized and Unauthorized Activities

Your computer is the property of the U.S. Government and it is to be used exclusively for official government business.

Identify requirements to Workgroup Manager before installing any software on your computer.

Software may be loaded onto a government computer with approval by the DAA, in coordination with the Network Control Center.

Maintain original software in a secure location such as a locked cabinet or drawer.

The Network Control Center supports software listed in the Joint Technical Architecture-Air Force (JTA-AF), examples include:

Operating Systems (Winxx, WinNT, UNIX, etc.)

Applications: (Outlook Client, Office 97, Adobe Acrobat Reader, etc.)

Utilities: (Norton Anti-Virus, McAfee VirusScan, etc.)

The following activities are unauthorized:

Any use other than for official and authorized business.

Activities for personal or commercial gain.

Storing or displaying offensive or obscene language or material, such as racist literature or sexually harassing or obscene materials.

Storing or processing classified information on any system not approved for classified processing.

Improperly storing or processing copyrighted material.

Viewing, changing, or deleting files of another user without appropriate authorization or permission.

Attempting to defeat security systems.

Obtaining, installing, copying or using software in violation of the license agreement of the vendor.

Permitting any unauthorized individual access to a government-owned or government-operated system.

Modifying or altering your software or hardware on your system.

Regardless of the sensitivity or classification of information, the following steps must always be performed:

Safeguard each information system and the information against sabotage, tampering, denial of service, espionage, or release to unauthorized persons.

Protect hardware, software, and documentation at the highest level of classification residing on the information system.

Report information systems security incidents, vulnerabilities, and virus attacks.

Virus Detection and Protection

Malicious Logic Protection:

Every user is responsible to protect information systems (including network servers) from malicious logic (such as viruses, worms, Trojan Horses, etc) attacks.

Users and system administrators should apply an appropriate mix of preventive measures to include user awareness training, local policies, configuration management, and anti-virus software.

What is a Virus?

A virus is a self-replicating, malicious program segment that attaches itself to an application program or another system component and leaves no obvious signs of having been there.

A virus is foreign information/data inserted into a system that causes destruction, scrambling or changing of internal operational data or output data transported to exterior devices, or other files within the system.

A virus is a software program written specifically to infect and alter other computer programs. It can easily infect the software or hardware on the system.

How are viruses spread?

Viruses are normally spread from one computer system to another via introduction of the virus into a network, via floppy disks processed on an infected system and then exported to other computers, or imported by external files from downloads.

Viruses can be received from diskettes, E-mail attachments (especially Word and Excel documents), and programs downloaded and executed. Viruses are known as malicious logic.

Occasionally, you will receive an E-Mail warning you of a potential virus or telling you to forward an E-Mail for some other reason. Do not forward E-Mails regarding virus alerts or chain letters. The majority of these E-Mails are not true and will clog up the network. If you do receive an E-Mail of this nature, contact your Workgroup Manager for guidance.

Disks containing new or updated software sometimes distribute viruses.

Here are a few examples of what to look for as indicators to alert you to the possibility of a virus hiding in your computer:

File abnormalities:

Files may increase, grow in size, or create modifications of data.

Unexplained filenames appear.

New data appears in stored files.

Files lost without reason or cannot be saved.

A file was copied without your invoking the command.

Files become corrupt or show incomplete data.

System abnormalities:

Unexpected decreases in the amount of random access memory space.

A disk light is on when not reading or writing to the disk.

Saving the working data does not appear to speed up operations.

System operates slowly.

Sudden lack of disk space or cannot access disk.

Appearance of unexpected messages, such as foreign messages or default messages generated by the computer.

Difficulty in printing and printing errors may occur.

Protection against viruses

There are four steps to protection: 1) Prevention, 2) Detection, 3) Eradication, and 4) Reporting.

1) Preventing Viruses:

Prevention is the single, most effective, and easiest approach for preventing system virus infections.

The keys to protecting against viruses are education and awareness, coupled with a disciplined practice of prevention procedures by all user personnel.

One way to prevent virus infections is to use magnetic media (such as floppy disks, CD-ROMs, 8mm tapes, etc.) that has been virus-scanned.

Use only AF-approved anti-virus software.

Install updates and upgrades to anti-virus software immediately.

For added protection, write-protect floppy diskettes when applicable and back up your data periodically.

Downloading files:

Virus-check all downloaded files, including sound and video files as well as E-Mail attachments.

To prevent the possibility of rapidly spreading a virus, do not download files to a network or shared drive.

2) Detecting viruses:

Anticipate that viruses might reach the systems within your organization, making detection an important component of system security.

Enable the Auto-Protect feature of your anti-virus software.

Watch for file or system abnormalities that may indicate a virus is present.

3) Eradicating viruses: Two easy items to remember in eradicating viruses are:

If your anti-virus software detects a virus, follow the steps identified by the anti-virus software program to get rid of the virus. Contact your Workgroup Manager for assistance.

Notify the initial sender of the virus.

4) Reporting viruses:

If your anti-virus software is unable to detect the virus and you believe you may have a virus, due to file or system abnormalities, contact your Workgroup Manager.

Backup Strategy

Why backup your data?

Backup copies are essential for recovery if working copies become defective. Keep in mind that backup media itself can fail.

Conduct backup operations as often as required based on the operational need and sensitivity of your information.

Also, having backup copies of files allows you to continue to work on files, when the network is unavailable.

Replace worn backup media immediately.

Data Backup:

Store backup media in a separate location from working media.

Paramount to limiting loss of critical information is routine backup of critical data and programs.

Keep several generations of backup files.

Keep a log of when each generation is made. When restoring from backup files, make sure archive files are not virus-infected.

Computer Security Controls

User Responsibilities:

There are several things you can do to ensure proper computer security controls, such as:

Never leave your computer unprotected while logged in.

Enable the password protected screensaver on your computer and/or employ physical measures (lock keyboard or door) before leaving the computer unattended.

Ensure your screensaver cannot be defeated by keyboard manipulation. If your system does not have a screensaver, log off the network. Contact your Workgroup Manager for assistance.

When in doubt--log out!

Password Policies:

Password security begins with each and every user.

Password security is strengthened when attention is paid to how passwords are composed.

Passwords must be at least eight characters long.

Passwords must be composed of all of the following:

Both numbers and letters...both upper and lower case letters...at least one special character such as: ~!@#\$\$%^&*()+

Do not construct passwords related to: your personal history, identity, job or environment.

Never use dictionary words, either forwards or backwards.

Placing a single number at the beginning or ending of a password does not prevent it from being cracked.

Most password cracking programs will check for and crack these passwords.

Please be aware the Network Control Center runs an automated vulnerability software, which checks for ineffective passwords. Any user whose password does not meet Air Force criteria will be directed to change their password.

Passwords must be changed at least every 90 days. Do not use former passwords for at least 6 months.

Passwords Lockouts

Your account will be locked out after three consecutive failed logon attempts. Contact your Workgroup Manager to unlock the account or to obtain a new password. You will not be given a new password without positive identification.

Password Protection

Each user is responsible and accountable for their password.

Do not share passwords with others.

Memorize your password.

Do not write down your password.

If documentation is necessary for mission accomplishment, place the password in a sealed envelope and lock in an appropriate container.

Protect the password to the same classification level of the system it is used on for example, if the system is Secret, then the password must be protected at the Secret classification level. At a minimum, protect passwords as For Official Use Only (FOUO).

Do not give your passwords over an unsecure phone line.

When entering your password, do so in such a manner that the password is not revealed to anyone observing you.

Remember: No one should ever ask you for your password! If anyone contacts you and asks for your password, report this incident to your Workgroup Manager immediately.

Summary

Your computer is the property of the U.S. Government and it is to be used exclusively for official government business.

Load only software supported by the Network Control Center (NCC) on government systems.

Be aware of unauthorized and prohibited activities involving use of computer hardware and software.

Malicious logic is hardware and/or software in systems that causes destruction, scrambling or changing of internal operational data or output data transported to exterior devices or other files within the system.

The four steps to virus protection are prevention, detection, eradication, and reporting.

It is important to backup your data to ensure recovery if working copies become defective. Accomplish backups depending on the criticality of the data.

Password protection is vital in securing your computer. Several guidelines should be employed when constructing your password; such as using both upper and lower case letters, at least one special character, and at least 8 characters in length. Additionally, passwords must be changed at least every 90 days and do not use former passwords for at least 6 months.

Password Management Quick Reference Sheet

The “DOs” of Password Management. Do:

- Use a combination of letters, numbers, and special characters.
- Mix the use of upper and lower case characters.
- Make the password pronounceable for easy memorization (for example, consonant-vowel-consonant).
- Use a length of eight or more characters in the password.
- Change your password every 60 to 90 days.
- Protect your password so you are the only one to know it.
- Enter the password carefully making sure nobody is watching.
- Use your account regularly to help you remember your password.
- Contact your CSSO if you suspect your password has been compromised.
- Make sure your password is not exposed on the screen during log-in.
- Verify the log-in information provided to make sure your account has not been used since your last session.

The “DON'Ts” of Password Management. Don't:

- Use a single word by itself for the password; especially ones from the dictionary, slang words, names, or profanity.
- Use words personally associated with you.
- Write down your password unless absolutely necessary; if written, protect it so you are the only one who knows it.
- Store your password on the desk, wall, terminal or in a function key or the communications software.
- Share your password with anyone.
- Let anyone watch you enter your password.
- Leave your terminal unprotected while you are logged in.

Appendix C: WIAT Course Exam

Available at <https://www.asc.wpafb.af.mil/base/c4/iaap/train/test.html>



*** This Test is for Wright-Patterson AFB Personnel only ***

* = required field

*Last Name:

*First Name:

*Rank: ▼

*Phone: Extension:

*Organization: ▼

*Type of Training:

Initial (New Account)

Refresher (Yearly Update)

Module 2, Computer Use

1. Software may be loaded on any government computer or system so long as it is:

a. mission critical

b. mission essential

c. certified by the Network Control Center

d. approved by the Designated Approval Authority

2. Original software must be maintained _____.

a. in a secure location

b. in a GSA approved container

c. and inventoried by the Network Control Center

d. and controlled by the Designated Approving Authority

3. When may government computers be used for other than official and authorized business?

- a. Never - this activity is prohibited
- b. So long as the work is mission critical
- c. After approval is received from the unit commander
- d. at any time when the system is not being used for official business

4. Which of the following activities is not prohibited?

- a. Activities for personal or commercial gain
- b. Storing or displaying offensive or obscene language or material, such as racist literature or sexually harassing or obscene materials
- c. Storing or processing classified information on any system not approved for classified processing
- d. All of the above activities are prohibited

5. You may permit an unauthorized individual access to a government -owned or government operated system so long as the work being done is mission essential and you have received prior approval.

- a. True
- b. False

6. Identify the steps that must always be performed, regardless of the sensitivity or classification of information.

- a. Report information systems security incidents, vulnerabilities, and virus attacks
- b. Protect hardware, software, and documentation at the highest level of classification resident on the information system
- c. Safeguard each information system and its information against sabotage, tampering, denial of service.
- d. All of the above

7. All users are responsible for reporting information systems security incidents, vulnerabilities, and virus attacks.

- a. True
- b. False

8. When is it ok to give out your password?

- a. When your System Administrator or Work Group Manager needs access to your computer.
- b. Give to a co-worker while you are on vacation.

- c. Never, no one should ever ask you for your password.
 - d. Both A and B are correct.
-

9. How are viruses normally spread from one computer system to another?

- a. through introduction of the virus into the network
 - b. through floppy disks processed on an infected system
 - c. imported by external files from internet downloads
 - d. all of the above
-

10. Which of the following can be infected by a computer virus.

- a. system memory
 - b. partition table and boot sector
 - c. executable, overlay, and system files
 - d. all of the above
-

11. Viruses can be received from diskettes, E-Mail attachments, and programs downloaded and executed.

- a. True
 - b. False
-

12. Viruses are known as _____.

- a. physical logic
 - b. malicious logic
 - c. illogical programming
 - d. logical configuration
-

13. There are many varying indicators that will alert you to the possibility of a virus hiding in your computer. Which of the following is not an indicator?

- a. Corrupted files
 - b. An increase in file size
 - c. The system operates slowly and performance is sluggish
 - d. The system continually shuts down
-

14. Which of the following is not a sign that a virus is present?

- a. You are able to print to file
 - b. The system operates slowly
 - c. Files are missing, have increased in size, or are corrupt
 - d. There is a sudden lack of disk space or you cannot access a disk
-

15. The four steps to virus protection are _____.

- a. safety, awareness, education, and training
 - b. prevention, detection, education, and analysis
 - c. prevention, detection, eradication, and reporting
 - d. awareness, protection, eradication, and reporting
-

16. _____ is the single most effective and easiest approach for preventing system virus infections.

- a. Detection
 - b. Education
 - c. Awareness
 - d. Prevention
-

17. One way to provide added protection against viruses is to _____.

- a. write-protect floppy diskettes
 - b. save critical files on the server
 - c. change ownership of files regularly
 - d. never allow other users access to your files
-

18. Which of the following must users virus check in order to protect against downloading viruses from internet files?

- a. All sender E-Mail addresses as well as their files
 - b. The services and protocols of the originating source
 - c. Internet sites for adequate security prior to downloading files
 - d. Downloaded files such as sound and video files as well as files attached to E-Mails
-

19. To prevent the possibility of rapidly spreading a virus, do not download files _____.

- a. to a network or shared drive
- b. when performing your routine backup procedures

- c. without first saving all your open application and files
 - d. without express permission from the system administrator
-

20. Which of the following actions should you take when reporting a computer virus?

- a. contact your system security administrator for resolution
 - b. comply with local security procedures and disable the affected system
 - c. contact your Workgroup Manager for assistance in eliminating the virus and reporting the incident
 - d. first attempt to repair the damage, then contact your Workgroup Manager for reporting requirements
-

21. Why should you back up your system?

- a. The Air Force requires backups
 - b. Backups are part of a system administrator's duties
 - c. Backups are not really necessary until a disaster is suspected
 - d. Backup copies are essential for recovery if working copies become defective
-

22. Frequency of backups is based on _____.

- a. local needs outlined in the base security policy
 - b. the operational need and sensitivity of your information
 - c. requirements dictated by the current world security environment
 - d. requirements set in Department of Defense and Air Force policies
-

23. When restoring from back-up files, make sure _____.

- a. to inform all network users
 - b. you continue your backup plan
 - c. you virus check all current files
 - d. archived files are not virus infected
-

Submit Test

Appendix D: Web-based retest/survey (AF-wide NUL users)

Page 1



U.S. AIR FORCE

Air Force Network Security Survey
Primary Researcher:
Capt Matthew J. Imperial, AFIT/ENV



AF Survey Control Number (SCN) 02-116, expiration 1 March 2003

DIRECTIONS: Please take this survey all at once and answer all questions with **NO** supplemental material except for your own personal knowledge. The results of this study will in no way be linked to any individual. In addition, your individual responses will be kept confidential. No one in your organization will see your completed survey.

Anonymity is ensured!

This survey should take approximately 15-20 minutes to complete.

Participation is voluntary. No adverse action will be taken against any member who does not participate in this survey. You may notice that the multiple choice questions are similar to ones in the AFCA Network User Licensing CBT you recently took. That is purposeful; however, please do not use any information outside your own personal memory.

Please contact us at AF_Network_Security_Survey@afit.edu if you have questions about this survey. Thanks for your participation! Your contribution will help improve network security training programs force-wide!

Please first complete the following demographic questions:

1. What is your e-mail address? (tracking purposes only)	<input type="text"/>
2. What unit are you assigned to?	<input type="text"/>
3. What MAJCOM are you assigned to?	<input type="text"/>
4. What is your current grade or employee category?	<input type="text"/>
5. What is your Air Force Specialty Code (if not applicable skip)?	<input type="text"/>

6. What is the general field in which you work?

7. Do you work with Network/Information Security issues on a regular basis (weekly)?

8. What is your attained level of education?

9. The last time you took the AFCA Smartforce Network User Licensing Training course, did you first review the course material before taking the course test?

Continue

AF Survey Control Number (SCN) 02-116, expiration 1 March 2003

Page 2

AF Survey Control Number (SCN) 02-116, expiration 1 March 2003

**Please answer the following questions using no supplemental material.
Choose the one best answer for each.**

Note: This multiple choice section tests your knowledge of information/network security. There is 1 right answer for each question.

1. Software may be loaded on any government computer or system so long as it is:

- mission critical
 - mission essential
 - certified by the Network Control Center
 - approved by the Designated Approval Authority
-

2. Original software must be maintained _____.

- in a secure location
 - in a GSA approved container
 - and inventoried by the Network Control Center
 - and controlled by the Designated Approving Authority
-

3. When may government computers be used for other than official and authorized business?

- Never - this activity is prohibited
 - So long as the work is mission critical
 - After approval is received from the unit commander
 - at any time when the system is not being used for official business
-

4. Which of the following activities is not prohibited?

- Activities for personal or commercial gain
- Storing or displaying offensive or obscene language or material, such as racist literature or sexually harassing or obscene materials

- Storing or processing classified information on any system not approved for classified processing
 - All of the above activities are prohibited
-

5. You may permit an unauthorized individual access to a government-owned or government-operated system so long as the work being done is mission essential and you have received prior approval.

- True
 - False
-

6. Identify the steps that must always be performed, regardless of the sensitivity or classification of information.

- Report information systems security incidents, vulnerabilities, and virus attacks
 - Protect hardware, software, and documentation at the highest level of classification resident on the information system
 - Safeguard each information system and its information against sabotage, tampering, denial of service.
 - All of the above
-

7. All users are responsible for reporting information systems security incidents, vulnerabilities, and virus attacks.

- True
 - False
-

*8. What is a virus?

- Foreign information, data, or both that is inserted into a system and causes destruction, scrambling or changing of internal operational data
 - Output data transported to exterior devices or other files within the computer's system
 - Both of the above
 - Neither of the first two options
-

9. How are viruses normally spread from one computer system to another?

- through introduction of the virus into the network
 - through floppy disks processed on an infected system
 - imported by external files from internet downloads
 - all of the above
-

10. Which of the following can be infected by a computer virus.

- system memory
 - partition table and boot sector
 - executable, overlay, and system files
 - all of the above
-

11. Viruses can be received from diskettes, E-Mail attachments, and programs downloaded and executed.

- True
 - False
-

12. Viruses are known as _____.

- physical logic
 - malicious logic
 - illogical programming
 - logical configuration
-

13. There are many varying indicators that will alert you to the possibility of a virus hiding in your computer. Which of the following is not an indicator?

- Corrupted files
- An increase in file size
- The system operates slowly and performance is sluggish
- The system continually shuts down

14. Which of the following is not a sign that a virus is present?

- You are able to print to file
 - The system operates slowly
 - Files are missing, have increased in size, or are corrupt
 - There is a sudden lack of disk space or you cannot access a disk
-

15. The four steps to virus protection are _____.

- safety, awareness, education, and training
 - prevention, detection, education, and analysis
 - prevention, detection, eradication, and reporting
 - awareness, protection, eradication, and reporting
-

16. _____ is the single most effective and easiest approach for preventing system virus infections.

- Detection
 - Education
 - Awareness
 - Prevention
-

17. One way to provide added protection against viruses is to _____.

- write-protect floppy diskettes
 - save critical files on the server
 - change ownership of files regularly
 - never allow other users access to your files
-

18. Which of the following must users virus check in order to protect against downloading viruses from internet files?

- All sender E-Mail addresses as well as their files

- The services and protocols of the originating source
 - Internet sites for adequate security prior to downloading files
 - Downloaded files such as sound and video files as well as files attached to E-Mails
-

19. To prevent the possibility of rapidly spreading a virus, do not download files _____.

- to a network or shared drive
 - when performing your routine backup procedures
 - without first saving all your open application and files
 - without express permission from the system administrator
-

20. Which of the following actions should you take when reporting a computer virus?

- contact your system security administrator for resolution
 - comply with local security procedures and disable the affected system
 - contact your Workgroup Manager for assistance in eliminating the virus and reporting the incident
 - first attempt to repair the damage, then contact your Workgroup Manager for reporting requirements
-

21. Why should you back up your system?

- The Air Force requires backups
 - Backups are part of a system administrator's duties
 - Backups are not really necessary until a disaster is suspected
 - Backup copies are essential for recovery if working copies become defective
-

22. Frequency of backups is based on _____.

- local needs outlined in the base security policy
- the operational need and sensitivity of your information
- requirements dictated by the current world security environment

- requirements set in Department of Defense and Air Force policies
-

23. When restoring from back-up files, make sure _____.

- to inform all network users
 - you continue your backup plan
 - you virus check all current files
 - archived files are not virus infected
-

Please answer the following questions on your exposure/involvement in the following network/information security activities outside the AFCA Network User Licensing CBT. Choose the frequency that best describes your personal work-related encounters.

	annually	bi-annually (twice a year)	quarterly	monthly	weekly	daily	never
a. View posters on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. View videos on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c. Read/receive newsletters (electronic or paper) on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d. Read/receive articles on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e. Read/receive emails on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f. View military websites involving network / information security material	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
g. View non-military websites involving network / information security material	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	annually	bi-annually (twice a year)	quarterly	monthly	weekly	daily	never
h. Attend lectures on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
i. Attend workshops on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
j. Utilize computer software dealing with network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
k. Participate in hands-on practice of network / information security measures	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
l. Receive guidance from senior leaders on the importance of network / information security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
m. Considering all of above mediums and others not mentioned, how often are you exposed to network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The complete results of this study will be available in March 2003.
If you are interested in receiving an executive summary of the results via email,
check the following box

Thank you for your time in completing this survey.

When complete, please click on the *Submit Survey* button below.

If desired, use the box below to make comments regarding this survey, the AFCA
NUL CBT you've previously taken, or your local network and information security
training and awareness program. Thanks again.



AF Survey Control Number (SCN) 02-116, expiration 1 March 2003

Air Force Network Security Survey

Results

Congratulations, you passed the knowledge-based multiple choice section of the survey.

You answered 23 of 23 questions correctly.
Your percentage of correct answers was 100.

----- OR -----

Air Force Network Security Survey

Results

Sorry, you failed the knowledge-based multiple choice section of the survey.

You answered 13 of 23 questions correctly.
Your percentage of correct answers was 57.

We suggest reviewing local Information Assurance printed material.

Appendix E: Web-based retest/survey (WPAFB USC/WIAT users)

Page 1



U.S. AIR FORCE

WPAFB Network Security Survey

Primary Researcher:

Capt Matthew J. Imperial, AFIT/ENV



USAF SCN 02-116

DIRECTIONS: Please take this survey all at once and answer all questions with **NO** supplemental material except for your own personal knowledge. The results of this study will in no way be linked to any individual. In addition, your individual responses will be kept confidential. No one in your organization will see your completed survey.

Anonymity is ensured!

This survey should take approximately 15-20 minutes to complete.

Participation is voluntary. No adverse action will be taken against any member who does not participate in this survey. You may notice that the multiple choice questions are similar to ones in the network security course you recently took. That is purposeful; however, please do not use any information outside your own personal memory.

Please contact us at (WPAFB_Network_Security_Survey@afit.edu) if you have questions about this survey. Thanks for your participation! Your contribution will help improve network security training programs force-wide!

Please first complete the following demographic questions:

1. What is your e-mail address? (tracking purposes only)	<input type="text"/>
2. What unit are you assigned to?	<input type="text"/>
3. What MAJCOM are you assigned to?	<input type="text"/>
4. What is your current grade or employee category?	<input type="text"/>
5. What is your Air Force Specialty Code (if not applicable skip)?	<input type="text"/>

6. What is the general field in which you work?

7. Do you work with Network/Information Security issues on a regular basis (weekly)?

8. What is your attained level of education?

9. The last time you took the Network Security Training requirement for licensing you on the network (formerly referred to as SATE training) did you first review the course text before taking the course exam?

Continue

Page 2

AF Survey Control Number (SCN) 02-116, expiration 1 March 2003

**Please answer the following questions using no supplemental material.
Choose the one best answer for each.**

Note: This multiple choice section tests your knowledge of information/network security. There is 1 right answer for each question.

1. Software may be loaded on any government computer or system so long as it is:

- a. mission critical
 - b. mission essential
 - c. certified by the Network Control Center
 - d. approved by the Designated Approval Authority
-

2. Original software must be maintained _____.

- a. in a secure location
 - b. in a GSA approved container
 - c. and inventoried by the Network Control Center
 - d. and controlled by the Designated Approving Authority
-

3. When may government computers be used for other than official and authorized business?

- a. Never - this activity is prohibited
 - b. So long as the work is mission critical
 - c. After approval is received from the unit commander
 - d. at any time when the system is not being used for official business
-

4. Which of the following activities is not prohibited?

- a. Activities for personal or commercial gain
- b. Storing or displaying offensive or obscene language or material, such as racist literature or sexually harassing or obscene materials
- c. Storing or processing classified information on any system not approved for

classified processing

- d. All of the above activities are prohibited
-

5. You may permit an unauthorized individual access to a government-owned or government-operated system so long as the work being done is mission essential and you have received prior approval.

- a. True
 - b. False
-

6. Identify the steps that must always be performed, regardless of the sensitivity or classification of information.

- a. Report information systems security incidents, vulnerabilities, and virus attacks
 - b. Protect hardware, software, and documentation at the highest level of classification resident on the information system
 - c. Safeguard each information system and its information against sabotage, tampering, denial of service.
 - d. All of the above
-

7. All users are responsible for reporting information systems security incidents, vulnerabilities, and virus attacks.

- a. True
 - b. False
-

*8. When is it OK to give out your password?

- a. When your System Administrator or Work Group Manager needs access to your computer
 - b. Give to a co-worker while you are on vacation
 - c. Never, no one should ever ask you for your password
 - d. Both A and B are correct
-

9. How are viruses normally spread from one computer system to another?

- a. through introduction of the virus into the network
 - b. through floppy disks processed on an infected system
 - c. imported by external files from internet downloads
 - d. all of the above
-

10. Which of the following can be infected by a computer virus.

- a. system memory
 - b. partition table and boot sector
 - c. executable, overlay, and system files
 - d. all of the above
-

11. Viruses can be received from diskettes, E-Mail attachments, and programs downloaded and executed.

- a. True
 - b. False
-

12. Viruses are known as _____.

- a. physical logic
 - b. malicious logic
 - c. illogical programming
 - d. logical configuration
-

13. There are many varying indicators that will alert you to the possibility of a virus hiding in your computer. Which of the following is not an indicator?

- a. Corrupted files
- b. An increase in file size
- c. The system operates slowly and performance is sluggish
- d. The system continually shuts down

14. Which of the following is not a sign that a virus is present?

- a. You are able to print to file
 - b. The system operates slowly
 - c. Files are missing, have increased in size, or are corrupt
 - d. There is a sudden lack of disk space or you cannot access a disk
-

15. The four steps to virus protection are _____.

- a. safety, awareness, education, and training
 - b. prevention, detection, education, and analysis
 - c. prevention, detection, eradication, and reporting
 - d. awareness, protection, eradication, and reporting
-

16. _____ is the single most effective and easiest approach for preventing system virus infections.

- a. Detection
 - b. Education
 - c. Awareness
 - d. Prevention
-

17. One way to provide added protection against viruses is to _____.

- a. write-protect floppy diskettes
 - b. save critical files on the server
 - c. change ownership of files regularly
 - d. never allow other users access to your files
-

18. Which of the following must users virus check in order to protect against downloading viruses from internet files?

- a. All sender E-Mail addresses as well as their files

- b. The services and protocols of the originating source
 - c. Internet sites for adequate security prior to downloading files
 - d. Downloaded files such as sound and video files as well as files attached to E-Mails
-

19. To prevent the possibility of rapidly spreading a virus, do not download files _____.

- a. to a network or shared drive
 - b. when performing your routine backup procedures
 - c. without first saving all your open application and files
 - d. without express permission from the system administrator
-

20. Which of the following actions should you take when reporting a computer virus?

- a. contact your system security administrator for resolution
 - b. comply with local security procedures and disable the affected system
 - c. contact your Workgroup Manager for assistance in eliminating the virus and reporting the incident
 - d. first attempt to repair the damage, then contact your Workgroup Manager for reporting requirements
-

21. Why should you back up your system?

- a. The Air Force requires backups
 - b. Backups are part of a system administrator's duties
 - c. Backups are not really necessary until a disaster is suspected
 - d. Backup copies are essential for recovery if working copies become defective
-

22. Frequency of backups is based on _____.

- a. local needs outlined in the base security policy
- b. the operational need and sensitivity of your information
- c. requirements dictated by the current world security environment

- d. requirements set in Department of Defense and Air Force policies
-

23. When restoring from back-up files, make sure _____.

- a. to inform all network users
 - b. you continue your backup plan
 - c. you virus check all current files
 - d. archived files are not virus infected
-

Please answer the following questions on your exposure/involvement in the following network/information security activities outside the WPAFB WIAT Network User Licensing CBT (SATE Training). Choose the frequency that best describes your personal work-related encounters.

	annually	bi-annually (twice a year)	quarterly	monthly	weekly	daily	never
a. View posters on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. View videos on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c. Read/receive newsletters (electronic or paper) on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d. Read/receive articles on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e. Read/receive emails on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f. View military websites involving network / information security material	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
g. View non-military websites involving network / information security material	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	annually	bi-annually (twice a year)	quarterly	monthly	weekly	daily	never
h. Attend lectures on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
i. Attend workshops on network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
j. Utilize computer software dealing with network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
k. Participate in hands-on practice of network / information security measures	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
l. Receive guidance from senior leaders on the importance of network / information security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
m. Considering all of above mediums and others not mentioned, how often are you exposed to network / information security issues	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The complete results of this study will be available in March 2003.
If you are interested in receiving an executive summary of the results via email,
check the following box

Thank you for your time in completing this survey.

When complete, please click on the *Submit Survey* button below.

If desired, use the box below to make comments regarding this survey, the AFCA
NUL CBT you've previously taken, or your local network and information security
training and awareness program. Thanks again.



AF Survey Control Number (SCN) 02-116, expiration 1 March 2003

WPAFB Network Security Survey

Results

Congratulations, you passed the knowledge-based multiple choice section of the survey.

You answered 23 of 23 questions correctly.
Your percentage of correct answers was 100.

----- OR -----

WPAFB Network Security Survey

Results

Sorry, you failed the knowledge-based multiple choice section of the survey.

You answered 15 of 23 questions correctly.
Your percentage of correct answers was 65.

We suggest reviewing local Information Assurance printed material.

Appendix F. Email Participation Request

From: *AF_Network_Security_Survey / WPAFB_Network_Security_Survey*
Subject: *AFCA / WPAFB Network Security Training Survey*

Hi, we are the Network Security Research Team at the Air Force Institute of Technology (AFIT).

We are conducting crucial research into the area of end-user network security training and awareness. This research is sponsored by the Office of the Secretary of Defense - Defense-wide Information Assurance Program (OSD-DIAP) and the Air Force Communications Agency (AFCA). This research will be published in March 2003 in an AFIT Thesis.

Experts agree that the most integral part of information security is the individual, namely you. The Air Force implements a broad Information Assurance Education, Training, and Awareness program aimed at increasing knowledge and skills.

One part is the network user licensing (NUL) computer-based training (CBT) course. You may recall taking either the initial or annual refresher CBT. This course is required for you to activate/maintain your computer network user account.

In fact, you are being asked to participate in this online survey because you have recently taken the (*AFCA NUL CBT / User SATE CBT (USC) followed by the WPAFB Information Assurance Test (WIAT) course*) (within the last 8 months).

Please help us in assessing the effectiveness of the network security training you received through the CBT as well as the overall robustness of your local network and information security training and awareness program. Your participation is voluntary. In participating, you will help strengthen Air Force information systems security and further protect them from adversaries by helping us better understand the effectiveness of current programs. After all, **you** are the most important link.

The survey is web-based and easy to navigate. It has been approved by the Air Force Personnel Center (AFPC), Survey Control Number 02-116.

It is located at the following weblink:

http://en.afit.edu/ENV/AFCA_Network_Security_Survey/default.cfm (*NUL survey link*) /

http://en.afit.edu/env/wpafb_network_security_survey/default.cfm (*USC/WIAT survey link*)

Click on the above link or copy and paste it into your internet browser address line then hit return.

Thank you.

Sincerely,

Network Security Research Team
Air Force Institute of Technology
Wright-Patterson AFB, OH

Bibliography

- Aeronautical Systems Center Public Affairs (ASC PA). *Wright-Patterson Air Force Base Fact Sheet 2002*. Unpublished article. n. pag. (2002).
Available at
<https://ascpa.wpafb.af.mil/Docs/Fact%20Sheets/WPAFB%20FactSheet%202002.doc>
- Air Force Communications Agency (AFCA). *AFCA CBT website*. Unpublished article. n. page. <https://www.afca.scott.af.mil/cbt/>. Downloaded 29 November 2002.
- Air Force Personnel Center (AFPC). *AFPC Fact Sheet*. Unpublished article. n. pag. http://www.af.mil/news/factsheets/Air_Force_Personnel_Center.html. Downloaded 30 November 2002.
- Barron, Ann. "Designing Web-based Training," *British Journal of Educational Technology*, 29, 4: 355-370 (1998).
- Bigge, Morris L. and S. Samuel Shermis. *Learning Theories for Teachers, 6th edition*. New York: Longman Publishers, 1999.
- Boisvert, Lisa. "Web-based Learning, the Anytime Anywhere Classroom," *Information Systems Management*, 17, 1: 35-40 (Winter 2000).
- Brown, B.L. "Web-Based Training, ERIC Digest No. 218," Columbus: *ERIC Clearinghouse on Adult, Career, and Vocational Education*, Center on Education and Training for Employment, The Ohio State University, EDO-CE-00-218. (2000).
- Catenazzo, Barbara. "Information Assurance, the Second Job that Must Become Second Nature," *Systems Administration, Networking and Security (SANS Institute)*. 20 December 2000.
Available at http://rr.sans.org/securitybasics/info_assurance.php
- Clark, Richard E. "Six definitions of media in search of a theory," In Donald P. Ely and Barbara B. Minor (Eds.), *Educational Media and Technology Yearbook*: p 65-76. Libraries Unlimited, 1992.
- Department of the Air Force (DAF). *Air Force Defensive Counterinformation Operations*. AFD 10-20. Washington: HQ USAF, 1 October 1998.
- . *Information Assurance (IA) Awareness Program*. AFI 33-204. Washington: HQ USAF, 21 September 2001.

- . *Licensing Network Users and Certifying Network Professionals*. AFI 33-115v2. Washington: HQ USAF, 1 November 1999.
- Department of Defense (DoD). *Defensive Information Operations Implementation*. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01B. Washington: 22 August 1997.
- Desman, Mark B. *Building an Information Security Awareness Program*. Boca Raton, FL: Auerbach-Publications, 2002.
- DeVries, Yousri Eldin and Candace Wheeler. "The Interactivity Component of Distance Learning Implemented in an Art Studio Course," *Education*, 117, 2: 180-184 (1996).
- Dixon-Krauss, Lisbeth. *Vygotsky in the Classroom: Mediated Literacy Instruction and Assessment*. New York: Longman Publishers, 1996.
- Dooley, David. *Social Research Methods*. (4th edition). Upper Saddle River, NJ: Prentice Hall, 2001.
- Federal Information Security Assessment Framework (FISAF). Federal Chief Information Officer's Council. 30 September 2000 draft. Available at http://www.cio.gov/Documents/info_security_assessment_framework_Sept_2000.html
- Fletcher, J.D. "Does This Stuff Work? Some Findings from Applications of Technology to Education and Training," *Proceedings of Conference on Teacher Education and the Use of Technology Based Learning Systems*. Warrenton, VA: Society for Applied Learning Technology, 1996.
- Fletcher, J.D. "Is it worth it? Some comments on research and technology in assessment and instruction," *Technology and Assessment Thinking Ahead Proceedings from a Workshop, Center for Education*, 2002. Available at <http://www.nap.edu/openbook/0309083206/html/26.html>
- Fletcher, J. Dexter and Marty R. Rockway. "Computer-Based Training in the Military," in John A. Ellis (Ed.), *Military Contributions to Instructional Technology*: p 171-213. NY: Praeger Publishers, 1986.
- Fox, Richard. "Constructivism Examined," *Oxford Review of Education*, 27, 1: 23-35 (2001).
- Haynie, W.J., III. "Effects of Anticipation of Tests on Delayed Retention Learning," *Journal of Technology Education*, 9, 1: 20-30 (1997).

- Hulse, Stewart H., Howard Egeth, and James Deese. *The Psychology of Learning, 5th Edition*. New York, NY: McGraw-Hill, 1980.
- Johnston, Rob B.E. *The Effectiveness of Computer-Based Training for Military Instruction: A Meta-Analysis*. A Thesis Presented to the School of Education, Drake University. May 1995.
- Jung, Insung, Seonghee Choi, Cheolil Lim, and Junghoon Leem. "Effects of Different Types of Interaction on Learning Achievement, Satisfaction and Participation in Web-Based Instruction," *Innovations in Education and Teaching International*, 39, 2: 153-162 (2002).
- Kabay, M. "Psychosocial factors in the implementation of information security policy," *EDPACS, The EDP Audit, Control, and Security Newsletter*, 21: Number 10: 1-10 (1994).
- Katsikas, Sokratis K. "Health care management and information systems security: awareness, training or education?" *International Journal of Medical Informatics*, 60: 129-135 (2000).
- Kerka, Sandra. "Interactive Video in Vocational Education. Overview. ERIC Digest No. 51," *ERIC Clearinghouse on Adult Career and Vocational Education*, ERIC Identifier ED268304, Columbus, OH (1986).
Available at http://www.ed.gov/databases/ERIC_Digests/ed268304.html
- Kettanurak, Vichuda (Nui), K. Ramamurthy, and William D. Haseman. "User attitude as a mediator of learning performance improvement in an interactive multimedia environment: an empirical investigation of the degree of interactivity and learning styles," *International Journal Human-Computer Studies*, 54: 541-583 (2001).
- Kulik, Chen-Lin C. and James A. Kulik. "Effectiveness of Computer-Based Instruction: An Updated Analysis," *Computers in Human Behavior*, 7: 75-94 (1991).
- Latham, Gary P. and Edwin A. Locke. "Goal Setting – A Motivational Technique that Works," *Organizational Dynamics*, 8, 2: 68-80 (1979).
- Maconachy, W.V. "Computer Security Education, Training, and Awareness: Turning a Philosophical Orientation into Practical Reality," *National Computer Security Center 12th National Computer Security Conference Proceedings*. (p 557A-557I). Alexandria VA: Defense Technical Information Center, 1989.
- Michas, Irene C. and Dianne C. Berry. "Learning a Procedural Task: Effectiveness of Multimedia Presentations," *Applied Cognitive Psychology*, 14: 555-575 (2000).

- Moll, Luis C. (Ed). *Vygotsky and Education*. Cambridge University Press, Cambridge, UK, 1990.
- Mucklow, Tim, Dr. *Information Technology courses go on line*. Air Force News, Air Force Communications Agency. Unpublished article. 29 June 2000.
Available at http://www.af.mil/news/Jun2000/n20000626_000965.html
- Muirhead, Brent. "Enhancing Social Interaction in Computer-Mediated Distance Education," *Ed at a Distance*, 15, 40 (April 2000).
Available at http://www.usdla.org/html/journal/APR01Issue/article_02.html.
- Nason, Captain Earl R. *A Survey of Air Force Computer-Based Training (CBT) Planning, Selection, and Implementation Issues*. Human Resources Directorate, Technical Training Research Division. Brooks AFB, TX. 1992.
- Niemiec, Richard and Herbert J. Walberg. "Comparative Effects of Computer-Assisted Instruction: A Synthesis of Reviews," *Journal of Educational Computing Research*, 3, 1: 19-37 (1987).
- North Western University (NWU). "Prophet Statguide: Does your data violate t test assumptions?" http://www.basic.nwu.edu/statguidefiles/ttest_unpaired_ass_viol.html#Non-normality. Evanston, IL: Downloaded 15 January 2003.
- Oliver, Ron, Jay Herrington, and Arshad Omari. "Creating Effective Instructional Materials for the World Wide Web," *The Second Australian World Wide Web Conference (AusWeb96)*. n. page. July 1996.
Available at <http://elmo.scu.edu.au/sponsored/ausweb/ausweb96/educn/oliver>
- Orlansky, Jesse and Joseph String. *Cost-Effectiveness of Computer-Based Instruction in Military Training*. Institute for Defense Analyses (IDA Paper P-1375). Arlington, VA: U.S. Government Printing Office, (April 1979).
- Perry, Neil R. and Jane S. Hemstritch. "Computer based training in the commercial sector," *Australian Journal of Educational Technology*, 2, 1: 33-41 (1986).
Available at <http://www.ascilite.org.au/ajet/ajet2/perry.html>
- Packer, Martin J. and Jesse Goicoechea. "Sociocultural and Constructivist Theories of Learning: Ontology, Not Just Epistemology," *Educational Psychologist*, 35, 4, 227-241 (2000).
- Paulsen, Morten F. *The Online Report on Pedagogical Techniques for Computer Mediated Communication*. Excerpt from online report. NKI, Oslo, Norway, n. pag. (August 1995).
Available at <http://www.nettskolen.com/pub/artikkel.xsql?artid=123#i>

- Public Law 100-235. *Computer Security Act of 1987*. H.R. 145. 9 January 1988.
Available at http://www.house.gov/science_democrats/archive/compsec1.htm
- Roberts, Bill. "E-Learning: New Twist on CBT," *HR Magazine*, p 99-106 (April 2001).
- Rodriguez, Rodolfo, MD, Efrain Campos-Sepulveda, Horacio Vidrio, MD, Eusebio Contreras, MD, and Fermin Valenzuela. "Evaluating Knowledge Retention of Third-year Medical Students Taught with an Innovative Pharmacology Program," *Academic Medicine*, 77, 6: 574-577 (June 2002).
- Rogers, Markus. Air Force Communications Agency, XPFT division, Scott Air Force Base, Illinois. Telephone interviews. July-November 2002.
- Rogoff, Barbara. *Apprenticeship in Thinking, Cognitive Development in Social Context*. Oxford University Press, New York, NY, 1990.
- Russell, Charles G. "Culture, Language and Behavior: Perception," *ETC*, p 4-27 (Spring 2000).
- Sanders, Raymond E., Debra J. Gonzalez, Martin D. Murphy, Bryan J. Pesta, and Barbara Bucur. "Training content variability and the effectiveness of learning: An adult age assessment," *Aging Neuropsychology and Cognition*, 9, 3: 157-174 (2002).
- Siponen, Mikko T. "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security*, 8, 1: 31-41 (2000).
- Spurling, Phil. "Promoting security awareness and commitment," *Information Management & Computer Security*, 3, 2: 20-26 (1995).
- Sutton, Leah A. "The Principle of Vicarious Interaction in Computer-Mediated Communications," *International Journal of Educational Telecommunications*, 7, 3: 223-242 (2001).
- Thomson, M.E. and R. von Solms. "Information security awareness: educating your users effectively," *Information Management & Computer Security*, 6, 2: 167-173 (1998).
- University of Southern California (USC). "Infosec Awareness, Training and Education," USC Office of Information Assurance and Center for Information Assurance Studies. Unpublished article. n. pag. Los Angeles CA: Downloaded 25 February 2002.
Available at <http://www.usc.edu/org/infosec/sate.html>.

- Vygotsky, L.S. *Mind in Society: The Development of Higher Psychological Processes*. Michael Cole, Vera John-Steiner, Sylvia Scribner, Ellen Souberman (Eds.), MA: Harvard University Press, (1978 translation).
- Vygotsky, L.S. *Thought and Language*. Alex Kozulin (Ed), MIT Press, Cambridge, MA, (1986 new revision of translation).
- Welch, B.L. "On the comparison of several mean values: An alternative approach," *Biometrika*, 38, 330-336 (1951).
- White, William F. "From S-R to S-O-R: "What every teacher should know," *Education*, 113, 4: 620-629 (Summer 1993).
- Wiggs, C.L. and R.J. Seidel. "An Overview of Computer-Based Instruction in Military Environments," In Robert J. Seidel and Peter D. Weddle (Eds.), *Computer-Based Instruction in Military Environments* (p 1-20). NY: Plenum Press, 1987.
- Williams, T. Craig and Hyder Zahed. "Computer-based training versus traditional lecture: Effect on learning and retention," *Journal of Business and Psychology*, 11, 2: 297-310 (Winter 1996).
- Wisher, Robert A., Christina K. Curnow, Robert J. Seidel. "Knowledge retention as a latent outcome measure in distance learning," *The American Journal of Distance Education*, 15, 3: 20-35 (2001).
- Wonacott, Michael E. *Web-Based Training and Constructivism, In Brief: Fast Facts for Policy and Practice No. 2*. National Dissemination Center for Career and Technical Education, The Ohio State University. Columbus, OH. 2000. Available at <http://www.nccte.org/publications/infosynthesis/in-brief/in-brief02/inbrief02-webtraining.pdf>
- Yildrem, Zahide, M. Yasar Ozden, and Medral Aksu. "Comparison of Hypermedia Learning and Traditional Instruction on Knowledge Acquisition and Retention," *The Journal of Educational Research*, 94, 4: 207-214 (March/April 2001).

Vita

Captain Matthew J. Imperial graduated from Washington Township High School in Sewell, New Jersey. He entered undergraduate studies at Villanova University, Villanova Pennsylvania where he graduated with a Bachelor of Science degree in Biology in May 1998. He was commissioned through Detachment 750 AFROTC at St. Joseph's University in Philadelphia, Pennsylvania.

His first assignment was to the 45th Space Wing located at Patrick AFB, Florida. He served as Chief of Communications Projects in the plans and programs branch of the 45th Communications Squadron and later as the Executive Officer of the 45th Logistics Group. As Executive Officer, he directly supported space launch activities at Cape Canaveral AFS for both manned and unmanned space vehicles as well as coordinated logistical and communication activities for the entire Eastern Range. In August 2001, he entered the Information Systems Management Master's Degree program in the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be assigned to the National Air and Space Intelligence Center at Wright Patterson AFB, Ohio.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 074-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 25-03-2003		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) Aug 2002 - Mar 2003	
4. TITLE AND SUBTITLE THE EFFECT OF INTERACTIVITY AND INSTRUCTIONAL EXPOSURE ON LEARNING EFFECTIVENESS AND KNOWLEDGE RETENTION: A COMPARATIVE STUDY OF TWO U.S. AIR FORCE COMPUTER-BASED TRAINING (CBT) COURSES FOR NETWORK USER LICENSING				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Imperial, Matthew J., Captain, USAF				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way, Building 640 WPAFB OH 45433-7765				8. PERFORMING ORGANIZATION REPORT NUMBER AFIT/GIR/ENV/03-07	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) OSD-DIAP AFCA 88 CG, WPAFB, AFMC Attn: Mr. George Bieber Mr. Markus Rogers Mr. Ben Striks Defense-wide IA Program (DIAP) AFCA/XPFT 88 CG/SCS 1215 Jefferson Davis Hwy 203 West Losey Street 2435 5th Street Suite 1101 Scott AFB, IL 62225 WPAFB, OH 45433 Arlington, VA 22202-4302 DSN 332-9980 DSN 779-5698 DSN 785-1294 email: george.bieber@osd.mil markus.rogers@scott.af.mil ben.striks@wpafb.af.mil				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The United States Air Force (USAF) currently employs the use of computer-based training (CBT) across a host of requirements. One such requirement is in the Information Assurance (IA) arena and involves the training/licensing of over one-million computer network end-users. USAF use of CBTs has been shown to possess a potential for substantial fiscal savings. However, studies investigating the learning outcomes of learning effectiveness (initial learning) and knowledge retention (sustained learning) associated with USAF CBTs are lacking. Currently, two USAF CBTs with sizeable user populations are used for the purpose of end-user network training/licensing: the Air Force Communications Agency's Network User Licensing (NUL) CBT and the Wright-Patterson Air Force Base (WPAFB) User SATE CBT / WPAFB Information Assurance Test (USC/WIAT). Interactivity has been described as one of the most important components of the learning experience (Jung et al., 2002). The primary design difference between the NUL and USC/WIAT CBTs was levels of interactivity - assessed as <i>Low</i> (NUL) and <i>None</i> (USC/WIAT). Utilizing a quasi-experimental method, this study analyzed the effects of interactivity on learning effectiveness and knowledge retention. Findings include support for a positive relationship between interactivity and knowledge retention. Interactivity was not shown to positively affect learning effectiveness but an exam implementation difference between the two CBTs, namely pass/fail thresholds, is theorized to have significantly increased learning effectiveness. Support for this claim is contained within goal-setting theories, which purport that when realistic and challenging goals are set, individuals strive to achieve those goals (Latham and Locke, 1984). The USAF also realizes that IA awareness and training should extend beyond CBTs and directs the implementation of a broad multifaceted strategy. Literature has stated that practice and learning that is related to, and occurs after, initial training can affect knowledge retention (Wisher et al, 2001). In this study, the concept of related practice/learning beyond CBTs is termed non-CBT instructional exposure and was assessed via a survey instrument. The effect of non-CBT instructional exposure on knowledge retention was also explored and evidence for a positive relationship between these two constructs was found. Other study contributions included significant practitioner-oriented findings. Support was found for fairly robust and diverse IA awareness and training programs both across WPAFB and the Air Force. Knowledge levels of end-users at the currently imposed one year retraining timeline were also assessed. The average of NUL new test scores at the one year point is projected to be 70.4 ± 4.5%, slightly above the 70% pass/fail threshold. The average of USC/WIAT new test scores at the one year point is projected to be 73.9 ± 4%, below the 83% pass/fail threshold. Recommendations for improving each CBTs design, implementation, and learning outcome results were also made and included: (1) an update/refresh of both CBTs' content and exams, (2) an increase in both CBTs' interactivity levels (3) an increase in pass/fail threshold for the NUL CBT, (4) the implementation of course testing controls for both CBTs, and (5) the use of existing and emerging adaptable learning technology platforms in future CBT versions.					
15. SUBJECT TERMS computer-based training, CBT, training, military training, air force training, computer aided instruction, programmed instruction, learning outcomes, interactivity, learning effectiveness, knowledge retention, instructional exposure, Information Assurance, IA, network user licensing, NUL, retraining timelines, pass/fail threshold, U.S. Air Force, USAF, web-based training, WBT					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Mark A. Ward, Major, USAF (ENV)
U	U	U	UU	176	19b. TELEPHONE NUMBER (Include area code) (937) 255-3636 ext 4742; email: mark.ward@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18