



Nova Southeastern University
NSUWorks

CEC Theses and Dissertations

College of Engineering and Computing

2007

Measuring the Effect of E-Learning on Job Performance

Heidi Kramer

Nova Southeastern University, kramerj64@aol.com

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

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



Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

NSUWorks Citation

Heidi Kramer. 2007. *Measuring the Effect of E-Learning on Job Performance*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (648) http://nsuworks.nova.edu/gscis_etd/648.

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

Measuring the Effect of E-Learning on Job Performance

By

Heidi Kramer

A dissertation submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Computing Technology in Education

Graduate School of Computer and Information Sciences
Nova Southeastern University

2007

UMI Number: 3288849

Copyright 2008 by
Kramer, Heidi

All rights reserved.

UMI[®]

UMI Microform 3288849

Copyright 2008 by ProQuest Information and Learning Company.
All rights reserved. This microform edition is protected against
unauthorized copying under Title 17, United States Code.

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

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

Gertrude W. Abramson, Ed.D.
Chairperson of Dissertation Committee

Date

Helen St. Aubin, Ph.D.
Dissertation Committee Member

Date

Ling Wang, Ph.D.
Dissertation Committee Member

Date

Approved:

Edward Lieblein, Ph.D.
Dean

Date

Graduate School of Computer and Information Sciences
Nova Southeastern University

2007

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

Measuring the Effect of E-Learning on Job Performance

by
Heidi Kramer

2007

E-learning is becoming a leading delivery method in workplace-learning settings across organizations of various sectors and of varying sizes. The ultimate goal is to drive business results. Managers need to provide evidence of a positive impact on corporate strategy and investment objectives. If the business goal cannot be identified, there should be a query on why it is there in the first place. Transfer of the knowledge learned in the training session to the work situation is not built into most skills training delivery, especially those provided through e-learning. The outcomes and the effects of training on job performance are not measured because no method currently exists for credible evaluation. This problem exists across the Information Technology (IT) industry.

Constant IT innovation makes technical competencies a fundamental requirement and continuous IT skills training a necessity. The trainee may have acquired the appropriate new skill, but the work environment to which the employee returns may make practicing what was learned counterproductive. The goal of the dissertation was to produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies. The instrument will be valuable to industries with IT departments.

The methodology for this study followed the Kirkpatrick Model, specifically Level 3, an evaluation that measures behavioral change on the job. The evaluation included specific application of the special knowledge or skills learned in the training. IT employees were surveyed after the completion of an online training class. The results indicated the frequency and effectiveness of the on-the-job application. In addition, open-ended questions provided feedback on the survey instrument and the training.

Utilized by corporations, the balanced scorecard approach was followed to track the alignment of online training with organizational goals. This approach includes a method to develop a measure such as strategy maps that depict overall organization strategic themes to improve the link between training and corporate strategy.

Acknowledgements

Completing this dissertation was a monumental task and there were many people who provided me with encouragement and support along the way. Those named below are only few.

My dissertation advisor, Dr. Trudy Abramson, showed me the way starting with our first meeting back in June 2002, which was before I even enrolled in the program. I would like to express my sincere and deepest appreciation for her mentorship, guidance and words of encouragement throughout the dissertation process. I would also like to thank my committee members Dr. Ling Wang and Dr. Helen St. Aubin. I am grateful to both of them for their critical appraisal of my work which ultimately led to a better product.

Special thanks go to my co-workers Mercy Torrente, Martha Percival and everyone who reviewed and participated in the survey. Roland Miller devised the survey and I am sincerely grateful for his willingness to help me.

My friends have always been important to me and their support of my endeavors means so much. Thanks to Nancy Friedman, Lauren Covitz and Carolyn Roth for always lending an ear even when I know you had better things to do.

To my parents, Sherwin and Harriet Handmacher, I thank you for always supporting my dreams. You have given me the tools I need to become successful and I will be forever grateful. To my sister, Wendy Firtell, I am very lucky to have you as a sister. I never doubted that for one second.

To my babies, Ryan and Jordan, who grew up during the years I was hidden behind my computer screen, I am so proud of the people you have become. And last but certainly not least, my deepest gratitude goes to my husband Jeffrey. I admire your patience, willingness to read through my work, constant words of encouragement and understanding of missing family events to work on my paper. It was your steadfast belief that it was *when* not *if* I complete my dissertation that kept me motivated.

Table of Contents

Abstract	iii
Acknowledgments	iv
List of Tables	vii

Chapters

1. Introduction 1

Background	1
Problem Statement	4
Dissertation Goal	5
Research Questions	6
Relevance and Significance	7
Barriers and Issues	8
Definitions of Terms	9
Summary	10

2. Review of the Literature 12

Overview	12
Corporate E-learning	13
Return on Investment for E-learning	15
Models for Evaluation of Training	17
Measuring the Relationship between Training and Job Performance	24
Business Metrics and Evaluation	28
E-learning Issues	30
Summary	35
The Contribution of the Study to the Field	35

3. Methodology 36

Introduction	36
Research Methods Employed	37
Quantitative and Qualitative	38
Reliability Testing	39
Validity Testing	41
Data Collection Procedures and Analysis	44
Analysis Prior to Survey Creation	46
Formats for Presenting Results	48
Resources Used	49
Summary	49

4. Results 51

Findings and Data Analysis 51

Summary 68

5. Conclusion, Implications, Recommendations, and Summary 70

Introduction 70

Conclusions 70

 Research Question 1 70

 Research Question 2 73

 Research Question 3 75

Limitations of the Study 77

Implications 78

Recommendations 79

 Recommendations for the Information Security Survey Instrument 79

 Recommendations for Practice 81

 Recommendations for Future Studies 86

Summary 87

Appendixes

A. Sample Impact Questionnaire 92

B. Information Security Awareness Training Survey 99

C. Institutional Review Board Approval 106

D. Survey Consent Letter 107

E. Results and Responses of Survey Question #8 108

F. Responses of Survey Question #9 113

G. Responses of Survey Question #10 117

H. Responses of Survey Question #12 121

I. Responses of Survey Question #13 122

J. Responses of Survey Question #14 126

K. Responses of Survey Question #16 128

L. Responses of Survey Question #17 130

M. Responses of Survey Question #18 132

Reference List 134

List of Tables

Tables

1. Training Evaluation Methods 17
2. Principal Components Analysis of the Six Subquestions of Question 2 44
3. Supervisory or Managerial Role 49
4. Objective of the Information Security Awareness Training 54
5. Implementation of On-the-job Actions Plans 55
6. Level of Improvement – Company Policies 56
7. Level of Improvement – Passwords and Social Engineering 57
8. Level of Improvement – Viruses, Worms, Adware and Spyware 58
9. Level of Improvement – Data Protection 59
10. Skills Most Aware of as a Result of the Training 60
11. Training as a Good Investment for the Company 62
12. Barriers Preventing Participant from Using the Skills 64
13. Supervisor Follow-up Discussions 66
14. Additional Support 66
15. Creating a Strategic Theme 73
16. Common Intangible Benefits 76
17. Creating a Strategic Sub-Theme 81
18. Aligning Training with Organization Goals 83
19. Presenting Corporate Strategies for E-learning Format 84

Chapter 1

Introduction

Background

Information Technology (IT) service departments continually face the challenge of how to train employees in an ever-changing technology world. Davaraj and Babu (2004) concede that organizations increasingly recognize that formal training is critical not only to the success of their software professionals but to their competitive position in the marketplace. Consequently, increasing pressure is put upon training departments to deliver high-quality training and education. While the training of technical employees is not a new challenge, measuring training for effectiveness and efficiency remains a daunting task. As companies continue to look for ways to cut costs, training departments will need to be able to show what is being done to support corporate objectives and to benefit the company.

Online learning (also known as e-learning) is becoming a dominant delivery method in workplace-learning settings across organizations of various sectors and of varying sizes. LeRouge and Webb (2003) assert that complex training technologies are increasingly used for IT staff to address time constraints, distance, simulated reality, and “just-in-time” training. Kim, Bonk and Zeng (2005) found that organizations spend between one and 60% of their total training budget on e-learning. Moreover, 25% of the respondents indicated that, in 2004, e-learning was already the dominant form of training in their organization, while another 50% predicted that e-learning would become the dominant form of training within their organization by 2010.

According to Van Dam (2003), the first wave of e-learning occurred in 1995. The second wave can be viewed from the perspectives of aligning online training with the business, e-learning solutions and deployment. E-learning will provide an opportunity to build key relationships within companies and build credibility as knowledge organizations.

The ultimate goal of effective e-learning is to drive business results. Corporate performance can be enhanced through alignment of training and business strategy (Beamish, Armistead, Watkinson, et al., 2002). Accordingly, managers need to demonstrate a positive impact on corporate strategy and investment objectives. If the business goal of a program cannot be identified, there should be a query on why it is there in the first place. According to Gale (2002), the ultimate value of e-learning comes when it is linked to achieving a company's goals.

Although the argument can be made that IT training is imperative and should be mandated throughout the department, superfluous training might not be beneficial to the company. Training and development that are not linked to improvement with the department and company are meaningless activities. Considering the dollars spent on IT training every year, a major question to be asked is whether there is an adequate return on investment. Large training budgets do not guarantee the adequacy of the IT skills among the company's workers. The State of the Industry Report (ASTD, 2006) declared the average annual expenditure per employee increased to \$1,424 per employee in 2005, an increase of 4% from 2004. According to Sugrue and Rivera (2005), typically these costs equate to 2% of payroll. Furthermore, the average number of hours of formal learning

per employee increased in 2005 to 41 hours per employee in 2005 (ASTD, 2006) up from 32 hours per employee in 2004 and 26 hours per employee in 2003.

Dagada and Jakovljevic (2004) envision that in the corporate training environment e-learning will ultimately become the new training paradigm, taking its place alongside traditional contact situation training and generally changing the face of training. However, the common theme in the literature suggests that work on e-learning strategies is neither well integrated nor focused on IT training, and thus, provides little direction to IT leadership (Olfman, Bostrom & Sein, 2003). Furthermore, Coverstone (2003) states that despite what would appear to be adequate training dollars expended, the degree of change in worker performance as a result of IT training, does not always meet management expectations.

The study focused specifically on e-learning for IT personnel of a utility company in Florida. IT personnel are computer professionals such as programmers, analysts, computer hardware maintenance specialists, database analysts, and other computer-related professionals. The company provides online learning opportunities, called the College of IM (information management) for these IT employees. There are over 1,500 courses across five critical technology subject areas: Software Development, Internet and Network Technologies, Operating Systems and Server Technologies, Enterprise Database Systems and Web Design. IT personnel were surveyed about their experiences with online training.

Problem Statement

Training is costly and a constant challenge in organizations since IT skills quickly become dated and competitive edge fades. In selecting training processes, companies find it difficult to ensure that their best interests are aligned with the needs of the employees. Bassi, Ludwig, McMurrer, and Van Buren (2000) state that there is a lack of a standard system for measuring and valuing training investments. Rewards for businesses and investors will come to those who pay more attention to the newly proven connection between training and bottom-line performance.

To respond to these changing times, there is a tilting of training toward online technologies. Sugrue and Rivera (2005) cite that the use of technology for delivering learning continued to increase from 24% in 2003 to 27% in 2004 and approximately 75% of the technology-based learning in 2004 was online. And while organizations invest heavily in IT training, Mahapatra and Lai (2005) observe that little effort is made to systematically evaluate the outcomes of the related programs and the effect of training on a trainee's job performance is rarely measured. Therefore, to decide whether and where to invest in e-learning, a thorough examination of the return on investment is indicated.

Coverstone (2003) and Davaraj and Babu (2004) address the effects of traditional training methods on IT staff performance. However, there are inadequate data on the effects of e-learning on IT staff. Olfman, Bostrom and Sein (2003) found that transfer of the knowledge learned in the training session to the work situation is not built into most IT skills training delivery, especially those provided through e-learning.

Montesino (2002) asserts that few studies have explored quantitatively the critical link between training and corporate strategy. His findings concluded with a low to

moderate positive correlation between the perceived alignment of training with the strategic direction of the organization. He suggests that in subsequent training programs, the company needs to pay close attention to linking its training programs with the corporation's strategic direction in a way that is explicit, clearly communicated, and evident to the trainees and their respective managers from the outset.

The investigator has held various IT positions in several companies over the course of 20 years. Currently, in an IT management position at a Florida utility company, she has found room for improvement in the execution of e-learning training. Her current employer has a mandate of 24 hours yearly minimum training for IT department employees. However, employees are not required to demonstrate added competencies after training. It would benefit the company to support a coordinated evaluation or assessment of IT training to determine return on investment and to guide future IT training requirements. Until this study, no formal or informal methods existed to evaluate training initiatives or to assess training outcomes.

The investigator's background and current employer provided the opportunity to solicit and understand the problem under investigation which is that there is no follow through process after e-learning training. The outcomes and the effects of training on job performance had not been measured because no method for credible evaluation was in place. The problem exists across the industry.

Dissertation Goal

Constant IT innovation makes technical competencies a fundamental requirement and continuous IT skills training a necessity. The trainee may have acquired the

appropriate new skill, but the work environment to which the employee returns may make practicing what was learned counterproductive (Coverstone, 2003). The goal of the dissertation was to produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies. The instrument will add to the return on investment (ROI) across similar industries.

ROI (Phillips & Stone, 2003) tries to determine if training had an effect on the business bottom line. Intangible data are data that either cannot or should not be converted to monetary values. For instance, potentially intangible benefits include increased organizational commitment, IT turnover reduction benefit, improved teamwork, and reduced stress. According to Potter (2000), retention is the top concern among IT organizations where turnover rates are between 11% and 20% and are predicted to continue.

Research Questions

The questions answered through this research are:

1. How must corporate strategies be presented so that they can guide the content and skills acquisition of e-learning?
2. How can the outcomes of training be measured to determine their effectiveness within the corporate strategies?
3. How can the evaluation process be used to increase tangible and intangible benefits to the organization?

Relevance and Significance

The need for developing employees to keep up with changes is growing as pressure is placed on the utility company for cost reductions. Given the current state of the recessionary economy, Feldman and Bahr (2004) emphasize that employee training and development are often the first costs to be cut in a downturn. The strategy that a corporation has towards its training can have an important impact on the overhead cost that the company incurs. Decisions involving training strategies can place a great importance on how to measure the value that training programs contribute to the bottom line.

Kraiger, McLinden and Casper (2004) state that one of the biggest reasons cited for not measuring performance or results is a lack of know-how. Half of the top 10 reasons that training evaluations fail was the lack of technical knowledge by training professionals regarding measurement and design. Wang and Li (2003) observe that the most frequent concerns in measuring training were the validity and reliability of available measures, isolating the impact of learning programs and a lack of knowledge about how to determine ROI.

Overall, the challenge of keeping employees technically skilled is not only important to IT departments and companies but to our country as a whole. With technology jobs continually lost to *out-shoring* (i.e., sending work to countries where wages are lower), the state of the country's economic strength is at stake. Although assessing the area of IT training seems relatively inconsequential in the scheme of things going on in the world, the implications are far-reaching including national security concerns. According to Feldman and Bahr (2004), software code development by some

offshore providers has already stirred security concerns. The inclusion of malicious programming code, coding mistakes and poor coding practices all make software users vulnerable to America's adversaries.

The results of this study will be beneficial to decision makers at the utility company and across corporate training programs regarding training budget and strategic decisions. The study was designed to advance knowledge and improve professional practice by providing a method to evaluate the alignment of corporate strategies and e-learning.

Barriers and Issues

Bassi, Ludwig, McMurrer, and Van Buren (2000) found two key obstacles in organizations' training investments. The first obstacle is a lack of a standard system for measuring and valuing training investments. The second obstacle is that the financial accounting and reporting structure in many organizations regard training as a cost rather than an investment.

Customer satisfaction surveys are considered simple lower level evaluations and are the most typically used for measuring training in organizations (Potter, 2000). There are reasons why organizations do not fully implement the higher level in-depth evaluations which are needed in order to analyze ROI. Bergman and Jacobson (2000) report four of these reasons which are difficulty in determining the impact on financial performance, time required for a proper evaluation, inability to determine appropriate outcome measures and the cost of evaluation.

Definition of Terms

Balanced Scorecard (BSC): A popular tool that companies use to measure corporate strategy (Beasley, Chen, Karen, & Wright, 2006; Cross, 2001; Kirkpatrick & Kirkpatrick, 2005; Pyzdek, 2004). The sole purpose of the BSC is to isolate key elements that leverage overall corporate strategy. Each line in a typical BSC consists of the specific strategy, the category, a description of the measure, the actual measure, and the desired target.

Business Metrics: A business metric is any type of measurement used to gauge some quantifiable component of a company's performance, such as return on investment, employee and customer churn rates, or revenues (Bitpipe, 2006).

E-learning or Online Learning: Online learning refers to distance learning environments that use Internet and/or Web-based technologies to support the teaching and learning process. One important point to note is that online learning can be used synonymously with e-learning, e-training, cyber education, and other similar and emergent constructs used to refer to Internet or Web-based learning, instruction, and education (Dabbagh & Bannan-Ritland, 2005).

Evaluation: A systematic process for ascertaining whether learning has been successful from performance, investment, and business perspectives.

Information Technology (IT) Personnel: IT workers are those persons engaged primarily in the conception, design, development, adaptation, implementation, deployment, training, support, documentation, and management of systems, components, or applications (Burnett & Subramaniam, 2004). For this study, IT workers include all

persons involved in computer occupations such as computer programmers, computer scientists, and system analysts.

Kirkpatrick Level 3 Evaluation: Kirkpatrick (1998) described four levels of evaluation that measure the effects of the training program on a trainee's job performance. These data address the transfer of training. A complete description is presented in chapter two.

Email SPAM: This is also known as bulk email or junk email that involves sending nearly identical messages to numerous recipients by email.

Out-shoring or Outsourcing: IT outsourcing means that the physical and/or human resources related to an organization's information technologies are supplied and/or administered by an external specialized provider. IT outsourcing is often more efficient than developing systems internally because production costs are lower with outsourcing. The provider obtains scale economies from mass-producing its services and distributing its fixed costs among a great number of end-user clients. Outsourcing IT can include data centers, wide area networks, applications development and maintenance functions, end-user computing and business processing (Paisittanand & Olson, 2006).

Summary

There are inadequate data on the effects of e-training on IT staff. This study conducted an in-depth evaluation. It examined the application and implementation of IT e-learning to determine whether participants actually applied what they learned from the training to their work settings. Also examined was whether actual business results were achieved as a consequence of applying the knowledge and skills. The overall goal was to

produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies.

Chapter 2

Review of the Literature

Overview

A review of the literature highlighted a number of different areas where e-learning has an effect on job performance. The fields of e-learning that are relevant to the dissertation are:

- 1) corporate e-learning,
- 2) return on investment (ROI) for e-learning,
- 3) measuring the relationship between training and job performance,
- 4) business metrics and evaluation,
- 5) models of evaluation of training, and
- 6) e-learning issues.

Literature on corporate e-learning and ROI for e-learning offered insight into how businesses support the e-learning infrastructure and how they view the payback of the training and bottom line savings to the company. Measuring the relationship between training and job performance is the key to understanding employees' behavior and whether or not trainees apply what they have learned. Business metrics and evaluation of training focus on various measures that companies utilize to determine the value of their training programs. The models for evaluation of training section highlight a few different methodologies commonly used for training evaluation. Finally, e-learning issues emphasize the fact that this field is still in its infancy.

Corporate E-learning

E-learning continues to grow in importance for corporate adoption. On any day, at least one million people in the U.S. are online taking a course (Kazmer & Haythornthwaite, 2004). According to Broad (2005), the primary feature of e-learning is the electronic linking of an instructor, remote in distance and/or time, and a performer and other stakeholders. Filho (2005) contends that most companies have built an e-learning infrastructure and extended it across the enterprise. E-learning can generate revenue; make relationships more productive with partners, suppliers and customers; and support key processes, such as compliance. To gain these benefits, however, the training department, IT organization and business units must jointly manage the business initiatives that e-learning supports. Training can no longer remain a stand-alone function.

In March 2007, Microsoft Chairman Bill Gates addressed the United States Senate Committee on Health, Education, Welfare, and Pensions about the need for improved workforce training (Microsoft, 2007). His two-hour testimony suggested that both private and public sectors must take responsibility to address the current and future skills gap in the American workforce. “As a nation, our goal should be to ensure that, by 2010, every job seeker, every displaced worker, and every individual in the U.S. workforce has access to the education and training needed to succeed in the knowledge economy. This means embracing the concept of *lifelong learning* as part of normal career path of American workers, so that they can use new technologies and meet new challenges. Workforce enhancement should be treated as a matter of national competitive survival.”

3Com, Bank One, Cisco Systems, Compaq, Dell, Domino's Pizza, Ecolab, GE Capital, IBM, Motorola, Rockwell Collins, and St. Paul Cos. are among the companies committed to e-learning programs that effectively address business challenges and performance improvement (Allen, 2003). Accordingly, several of these companies predict that within a few years, half of their training budgets will be devoted to e-learning. 3Com has already dedicated 75% of its training budget specifically to computer-based learning.

A Gartner survey (Eid, 2006) showed that two of the most significant reasons for investing in e-learning technologies are to move users toward a self-service model of information access and delivery and to align and track more closely with corporate strategy and objectives. According to Kirkpatrick and Hawk (2006), regardless of the learning media, there are four questions that must be answered before an effective evaluation can take place. First, what business results is the company looking for? Second, what new behaviors by course participants will be required to bring about those results? Third, what new knowledge, skills and attitudes will be required to bring about the new behaviors? And finally, what kind of reaction will be needed from the participants to set the stage for learning?

Evaluation and measurement are essential components of any effort to improve performance in organizations. According to Broad (2005), that is the only way to know whether training is effective in achieving learning, is well applied by transfer of learning to performance, and has the desired impact on organizational results. Stakeholders, including organization decision-makers, are giving growing attention to evaluation to

measure outcomes, particularly for expensive training interventions to improve workforce performance (Phillips & Stone, 2003).

Return on Investment (ROI) for E-learning

E-learning ROI is a vitally important topic within companies and training departments continually face challenges in making it relevant (Harris, 2003). Egan, Hessian, Taylor and Zenger (2003) claim that the first e-learning ROI rule is that *E* is for effectiveness. Moran (2002) claims that speed and efficiency are two factors that contribute to ROI and are reasons more compelling than dollars to move to e-learning. Speed is a well-known competitive advantage in business (Taylor, 2002), and according to various studies, it requires 25 to 60% less time to convey the same amount of learning online rather than in a classroom setting. Additionally, e-learning also offers instant scalability in that more employees can be trained in a shorter time, anywhere.

Harris (2003) has found that sometimes the adoption of e-learning is such an obvious choice and its benefits are so apparent that an ROI analysis seems to write itself. For instance, IBM (Mullich, 2004) discovered that managers who have been exposed to online computer training say that they never want to go back to classroom-only training. IBM found that using such technology has enabled the company to trim the cost of training by \$400 million a year. It currently conducts 48% of its training electronically. However, IBM has found that e-learning works most effectively when strategically coupled with classroom training.

International Data Corporation (Cross, 2001) studied the buying behavior of corporate and IT training managers and concluded that ROI will no longer be measured in savings or reduced cost of training. Instead, attention will be directed to measurable

changes to business metrics resulting from training investments. Those benefits will only emerge if vendors increase their focus on high-quality instructional design and engaging learning environments. Cross quoted an Information Week survey which revealed that more companies are justifying their e-business ventures not in terms of ROI but in terms of strategic goals. Creating or maintaining a competitive edge was cited most often as the reason for deploying an application. This is in line with the thinking of some training managers that the traditional concept of training ROI is obsolete. More managers are employing business metrics and time value more than traditional ROI and budgets.

As Reddy (2002) states, specifically with respect to e-learning, the requirement of ROI that all benefits be boiled down to a monetary figure is not an easy task. Even assuming that there is a significant transfer of the learning onto the job, a monetary ROI figure still ignores the impact of the state of the economy, competitors' products, any changes in the company's incentive structure, improvement in its own products, and the organization's revenues and profits. So it is not only unrealistic to try to isolate the impact of an e-learning initiative but possibly very time-consuming and expensive.

If managers want to take a look at budgets, there is another hidden cost savings associated with e-learning which is energy related. A recent study (Mulgan, 2006) found immense energy savings associated with online learning. Specifically, the study found that on average, the production and provision of distance learning courses consumed nearly 90% less energy and produced 85% fewer carbon dioxide emissions per student than conventional campus-based university courses. Mulgan took the findings and compared them as to how they might affect corporate training. The analysis found that there is a significant level of energy consumption due to the provision of live training and

that with the rising fuel costs and pressure to cut energy consumption, e-learning is an increasingly attractive as well as environmentally responsible choice.

Models for Evaluation of Training

Determining what to measure and why creates the foundation for moving forward with the selection of a methodology. Coverstone (2003) states that evaluation in the corporate world is most likely linked to the bottom line. Without evaluation it is not possible to know whether one's objectives are being met. In this section, different methods of training evaluation will be presented although it is important to note that this study will utilize the Kirkpatrick Level 3 methodology. Table 1 compares the evaluation models discussed in this section. The following paragraphs will present each method.

Table 1. Training Evaluation Methods

Methodology	Evaluation Elements	Objective
Kirkpatrick	Level 1 – Reaction Level 2 – Learning Level 3 – Behavior Level 4 – Business Results	Provides training data in four areas
Training for Impact	Identify Business Need and Client Form a collaborative relationship Conduct Initial Project Meeting Assessment Conduct Training Collect and Interpret Data Report to Client	Measure results of training in business
Success Case Method	Focus and Plan Study Create an Impact Model Design & Distribute a Survey Interview Prepare Report of Findings	Measure results of training in business to ensure alignment with organizational strategy
Kirkpatrick-Phillips	Level 1 – Reaction Level 2 – Learning Level 3 – Behavior Level 4 – Business Results Level 5 – Return on Investment	Adds a monetary value added verses cost comparison, called Return on Investment (ROI)

Kirkpatrick Four-Level Approach

One of the most widely reference models for training evaluation is the Kirkpatrick model (Broad, 2005; Coverstone, 2003; Galloway, 2005; Mahapatra & Lai, 2005; Potter, 2000). It is an outcome-based model defined by four levels: reaction, learning, behavior and results (Coverstone, 2003). According to Kirkpatrick (1998), each level adds information to create a comprehensive view of the value of the training program.

The four levels indicate a method for determining criteria about a training program. Level 1 measures the satisfaction of the trainee with the training material, instructor, instruction, and environment. Reactions data measure what the training participant think and feel about the training. Did they enjoy the training? Was it relevant to their job? Were the instructors interesting, knowledgeable, and prepared? Was the training organized well? Was adequate time allotted to training? Reaction data are typically collected by means of a questionnaire.

Level 2 measures how much the training participants increased their knowledge or skills. Learning data are typically collected by means of a pretest and a posttest designed to measure gain in the knowledge of the trainees due to the program. Level 2 measures should be as close as possible to the actual work performance and setting so that they accurately measure accomplishment of the desired knowledge and skills (Broad, 2005).

Level 3 measures the effect of the training program on the trainee's job performance. These data address the issue of *transfer of training*. The question to ask is if the participants are using what they have learned back on the job. Behavior data collection usually involves supervisors' observations and reports of on-the-job behavior.

According to Mayberry (2005), this level of evaluation will increase the visibility of learning and development efforts. Successful implementation of Level 3 evaluations affects learners, managers, project stakeholders, subject matter experts, and line supervisors. Level 3 evaluations may also relate to mentoring programs, annual performance reviews and development planning activities.

Level 4 measures the effect of the training program on overall organizational performance (Mahapatra & Lai, 2005). Results data measure the impact of training on organizational performance metrics such as improved productivity, increased sales, additional profit, increased market penetration, improved efficiency, higher quality, reduced turnover, reduced costs, reduced absenteeism and other factors. Overall, Kirkpatrick's (Ford, 2004) model implies that if participants react favorably to training, their learning should increase. If their learning increases, their job behavior should change. If their behavior changes, the organization should benefit from improved performance. If any of these linkages breaks down, that signifies a problem with the training implementation process. However, critics of the Kirkpatrick model, such as Ford and Holton (1996), challenge the validity of the causal link between reactions and learning. They have proven that good ratings at one level do not necessarily equate with learning new skills. Chevalier (2004) also argues that Level 1 and Level 2 evaluations can lead to a false sense of security. There may be no relationship between how participants feel about the training and improved individual and organizational performance. In any case, it may not be desirable, practical, or necessary to do all five levels of evaluation.

Although the Kirkpatrick model was originally designed to measure classroom training, trainers have bridged the evaluation model into the e-learning environment. Galloway (2005) contends that Level 3 has the potential of being more relevant to evaluating today's training (including e-learning) than it did when the model was first implemented in 1959 at which time technologies such as computers were less available to measure learning. Level 4 is often utilized by management because it produces evidence in terms of dollars that can be related to increased sales, reduced costs, increased productivity, improved quality, and lower overhead.

According to Horton (2005), e-learning can be evaluated using Kirkpatrick's tried-and-true levels of evaluation. In many situations, e-learning is a new experience for learners. Level 1 evaluations can help monitor learners' emotional acceptance of e-learning, and it can be essential in gathering the testimonials and statistics to generate a positive attitude around e-learning. E-learning greatly simplifies Level 2 evaluations. In e-learning, tests can be automatically administered, scored, recorded, and reported. Since a change in behavior occurs outside the e-learning experience, Level 3 evaluation is less associated with the e-learning or to the technologies needed for e-learning. However, electronic means of evaluation are likely to be economical to implement. Electronic questionnaires can be used to measure on-the-job performance. E-mail, online forms, and discussion forums can also be used to ask supervisors to appraise employees' progress on specific performance goals, and thereby measure whether distant learners have achieved these goals. Evaluating Level 4 results for e-learning is considerably more difficult than it is for classroom training. In some cases, it might be valuable to ask the

evaluator for an estimate of the monetary value of a change resulting in part from e-learning.

Training for Impact Model

Robinson and Robin (1989) have developed The Training for Impact Model, which emphasizes helping training coordinators understand how to be more successful within the organization they are supporting. Training programs must be tied to business needs, problems, or opportunities, and these links must be clearly understood by management. The training model consists of the following twelve steps:

1. Identify Business Need and Client
2. Form a Collaborative Relationship
3. Conduct Initial Project Meeting
4. Conduct Performance Assessment
5. Conduct Cause Analysis
6. Tabulate and Interpret Data
7. Report Results to Client
8. Design Evaluation System
9. Design Tracking System
10. Conduct Training
11. Collect, Tabulate, Interpret Data
12. Report to Client

The model lends itself to specific methods for quantifying the value of training to the business organization. A more recent discussion from Robinson and Robinson (2005) reinforces the importance of working with business leaders to influence strategies and directions for a particular business unit.

The Success Case Method

The Success Case Method (SCM) (Brinkerhoff, 2005) is a process for evaluating the business effect of training that is aligned with and fulfills the organizational strategy. According to Brinkerhoff, the SCM is relatively simple and can be implemented entirely in a short timeframe. It is intended to produce concrete evidence of the effect of training in ways that senior managers and others find highly believable and compelling.

Morrison (2004) describes the five steps of the SCM model. The first step is to focus and plan the study. The next step is to create an *impact model* that defines what success would look like if the initiative were met. The third step is to design and distribute a survey to search for best and worst cases of program success. The survey should ask for specific behavior not reactions or feelings. In the fourth step, the participants should be interviewed. The final step includes preparing a report of the findings, conclusions, and recommendations.

The results of a Success Case (Brinkerhoff, 2002) study are communicated in *story* form. The evaluator finds the most compelling and descriptive examples of success the program has achieved, then documents these examples in a few brief but richly detailed stories. The SCM model differs from typical more quantitative methods in that it does not seek to learn about the average participant in an initiative. It intentionally seeks

the very best that a program is producing to help determine if the value a program is capable of producing is worthwhile. The SCM model is similar to other evaluation approaches in that it uses many of the same tools of typical evaluation, such as survey, statistical analysis and interviewing. Overall, it is simpler and faster, but not as comprehensive as other evaluation methods.

Kirkpatrick-Phillips

The Kirkpatrick-Phillips model (also known as The Phillips Five-Level ROI Framework) takes Kirkpatrick's four level framework and adds a fifth level: ROI (Phillips & Stone, 2003). According to Ford (2004), this model is increasingly dominant in evaluation circles as pressure mounts to demonstrate the performance and financial results of training and performance improvement work. ROI measures the monetary value of the results and costs for the program and is usually presented as a percentage or benefit-cost ratio, in which monetary benefits are compared to cost to determine whether training costs were excessive. At the fourth level, results evaluate whether or not the training provided a business result. While some training professionals argue that measuring ROI for training is not possible (Galloway, 2005), there is general agreement that trainers must show an ROI so that funds will continue to be made available for training programs.

Phillips and Stone claim that the ROI model also focuses on the value of the training in non-monetary terms, called intangible benefits. Overton (2005) notes the importance of not ignoring the intangibles, such as less stress and improved job satisfaction, even though they are difficult to quantify. Furthermore, in an e-learning

environment, unique costs and benefits exist and must be accounted for in an accurate measure of ROI. For example, e-learning training and development typically involves reduced travel expense, reduced time away from the workplace, 24-hours, 7-day-a-week access to training, and possibly reduced turnover. In this way, e-learning's ROI can be defined in the same terms of dollars, benefits, and outcomes that define traditional learning (Galloway, 2005).

Measuring the relationship between training and job performance

It is widely assumed that Kirkpatrick Level 3 data are measures of the effectiveness of the training program (Broad, 2005). However, research (Broad, 2005; Broad & Newstrom, 1992) has shown that there are many factors in the organization and work environment that affect transfer of learning to job performance, only one of which is the quality of the training program. According to Kirkpatrick and Kirkpatrick (2005), there is nothing more important than measuring the extent that on-the-job behavior has changed as a result of the training. If the trainees do not apply what they learned, the program has been a failure even if learning has taken place. Therefore, measuring behavior change is necessary, not only to see if behavior has changed, but also to determine the reasons why change has not occurred.

Cross (2001) asserts that in order to prove beyond a shadow of a doubt that a given training program produced a given result is to link learning to business results. He suggests establishing a causal link between a particular skill deficiency and a particular business outcome. Kirkpatrick and Hawk (2006) agree that a challenge for all corporate universities and training departments is how to demonstrate the value of learning to

business executives. Identifying business needs and developing targeted learning opportunities are the core of ultimate strategic execution. The objectives for a particular course or program reflect what knowledge and skills a participant should gain in the course. Although it is easy to see there is a contribution, it is difficult to gather the evidence to demonstrate it.

Devaraj and Babu (2004) conducted a study to measure the relationship between training and job performance. They identified the drivers of job performance within Infosys, a major software industry service provider based in Bangalore, India. First, they looked at the appraisals reported by supervisors of on-the-job performance for employees who underwent a specific training. Then they calculated a grade point average to assess participants' performance on certain generic courses such as programming fundamentals, database management, and systems analysis and design. They were able to draw conclusions based on these data as to the employees' eventual performance on the job.

In an attempt to address training outcomes, the National Institute of Corrections Academy, as part of its delivery of the Management Development of the Future training program to the Utah Department of Corrections (DOC), has put into place a formal evaluation protocol based on Kirkpatrick's four levels of evaluating training programs (Brown & Eggers, 2005). This evaluation process was put into place because of their basic belief that if an individual cannot assess participant behavioral change and subsequent impact on the organization, there is no way to know if the program is making any difference. Accordingly, participants completed a Kirkpatrick Level 3 online questionnaire to rate themselves. They were also rated by the manager, direct reports, coworkers and others. The Level 3 questionnaire measures participant behavior.

Interestingly, one of the key performance indicators that the Utah DOC is addressing is employee turnover. If this variable can be decreased, the results can be measured in terms of dollar savings for the department.

Chevalier (2004) describes an example of how the Coast Guard Training Center in Petaluma, California used the Level 3 evaluation process. They have begun using an online survey of graduates and their supervisors and have seen more than a 65% return rate for the surveys. In this case, the value of Level 3 evaluation was in making training more efficient and effective by closing the feedback loop between the provider and the customer (graduates and supervisors). As a result of the systematic assessment, courses were continuously refined, allowing the training to be delivered more efficiently and making it more relevant. Student years of training were reduced as outdated objectives were eliminated and job aids were introduced.

Broad (2005) states that the work environment may not support the learning transfer. The manager or the company culture may not support the training due to lack of time, resources, or opportunity to use the skills. The trainees may see no need to apply what they learned or the reward systems do not support gaining new skills. Some managers believe they have nothing to do with training beyond freeing their reports for the time required to take the class. This indifferent attitude can sap enthusiasm for the training. Phillips and Stone (2003) recommend that managers should be held accountable for their role in the process. Various ways to involve managers are to participate in a needs assessment for target jobs in their area, serve as a subject-matter expert for a specific program, serve on a task force to develop training or allow a pilot test in their department.

Chevalier (2004) argues that while many organizations view evaluation as nice to have at best, managers need to learn that evaluation can be an important part of their overall intervention strategy. The act of measuring performance encourages the use of what has been learned in the training, as well as reinforces the desired change associated with other performance improvement initiatives. In addition, evaluation documents the impact that training has made and makes the training function more defensible during budget cuts and more credible when additional resources are requested.

Kirkpatrick and Kirkpatrick (2005) list the top 10 mistakes leaders make when trying to transfer learning to behavior. Most are errors of omission.

- (1) Not eliciting buy-in and involvement from executives.
- (2) Not following up and following through.
- (3) Not developing action plans from a business consulting approach.
- (4) Promoting a culture of employees who are discouraged from learning.
- (5) Not providing clear direction – vision, strategy, and expectations.
- (6) Not providing a balance of accountability and support.
- (7) Not providing adequate technology and system support.
- (8) Having the wrong kind of leaders or the right kind in the wrong positions.
- (9) Trying to do too much and not focusing efforts on mission critical behavior.
- (10) Not linking and aligning incentives to desired behavior and subsequent results.

Business Metrics and Evaluation

Krell (2002) investigated different companies to determine how they measure their e-learning ROI. In addition to cost, he found many other different tools and metrics were being utilized. For instance, the managing partner for e-learning and knowledge management with Accenture in Dallas identified four different areas that training managers should use when measuring the return on e-learning investments. First, the business function of training should ask the question, what is the efficiency and efficacy of knowledge acquisition within the context of the training function? Second, line management should ask the question, can employees perform better than they did so before the training? Third, business unit management should ask the question, what is the aggregate financial performance of the business units and how is the workforce performance improving those numbers? And finally, the executive team should ask the question, how is the organization performance and financial performance of the company based on a handful of high-level metrics like economic value added?

Krell's investigation also found that one of Cisco's, the leading supplier of networking equipment and network management for the Internet, most effective e-learning ROI measurement tools is the survey it distributes twice a year to its partners that rely on the company's e-learning portal. Cisco believes that accelerating their partners' ability to sell and service customers, increasing their productivity and satisfaction with the tool, and continuing to reduce costs are the key measurements. The survey is a measurement tool that helps crystallize those returns. Cisco also reports increased productivity resulting from e-learning, including reduction in support costs, improved efficiencies while using business tools, increased workloads while requiring

fewer people and quicker implementation of tools to a broader scope of employees (Hall & LeCavalier, 2000).

The balanced scorecard (BSC) is a popular tool that companies use to measure corporate strategy (Beasley, Chen, Karen & Wright, 2006; Cross, 2001; Kirkpatrick & Kirkpatrick, 2005; Pyzdek, 2004). Kaplan and Norton (as cited in Cross, 2001), developed the BSC as a means of evaluation to help make up for the insufficiencies of financial accounting. In addition to finances, the tool looks at changes in customers, processes, and employees. The method was designed to look backward however there is no reason not to use it to project into the future as a decision-making tool. Shell Oil Company (Hall & LeCavalier, 2000), for example, includes learning in all its business unit scorecards.

Kirkpatrick and Kirkpatrick (2005) have developed a step by step guide to depict how the BSC method can be used to determine the link between training and corporate strategies. The sole purpose of the BSC is to isolate key elements that leverage overall corporate strategy. Each line consists of the specific strategy, the category, a description of the measure, the actual measure, and the desired target.

One of the main reasons that training fails is because of the lack of alignment with the business needs (Kirkpatrick & Kirkpatrick, 2005). Traditionally, training professionals have focused on Kirkpatrick's Level 2 (learning) evaluation in their training needs assessments. However, Phillips and Stone (2003) contend that training professionals need to think about application of what is learned and changes in on-the-jobs behavior (Level 3) and business impact (Level 4) in the assessment process. Phillips and Stone suggest that training should be made part of an employee development plan to

provide reinforcement for applying the principles on the job. In addition, post-training coaching or on-the-job training should be included as part of the process. Other suggestions are to use posters or flyers to reinforce the desired business results, provide an online forum to continue a dialogue on the training among participants, and encourage managers to reinforce the training during staff meetings.

The American Society for Training and Development's (ASTD) 2003 State of the Industry Report provided the results of a benchmarking survey of 276 US organizations who reported the extent to which they evaluated their training programs at each of Kirkpatrick's four levels. A total of 75% evaluate their training programs to determine the participants' reaction (Level 1) and 41% report that they evaluate what knowledge and skills are learned (Level 2). Only 21% of those organizations surveyed report that they evaluate whether the behavior of the participants changes because of the training (Level 3), and only 11% evaluate whether training results in improved business results (Level 4). If anything, these figures are high for the training industry as a whole since these organizations were selected from those that voluntarily participate in the study each year.

E-learning Issues

Cost becomes a challenge in e-learning whether it is measured in terms of an expenditure or as a cost-savings to the company. According to Webb (2003), analysts, vendors and customers agree that the biggest obstacle to implementing large-scale e-learning initiatives is cost. Accordingly, Filho (2005) quotes a Gartner survey that found the budgeting process is often fragmented and results in needless costs.

Cross (2004) contends that executives assume training has little or no impact on revenue, so they measure training benefits in terms of cost savings. This works against e-learning in which increase in top-line revenue generally exceed reduced expenses by a wide margin. However, Bersin (2002) states that it is important to remember that the ultimate purpose of e-learning is not to reduce the cost of training, but to improve the way an organization does business. Overall, training professionals often do not like to acknowledge the historically low stature and importance that training and learning occupy within the corporate hierarchy because of the perceived difficulty of determining ROI for training activities (Galloway, 2005).

Cross (2004) communicates an interesting observation in that the largest overall cost of any corporate learning endeavor is the cost of people's time. This does not include salaries and benefits but the value they would have created had they not been tied up in training. Opportunity cost per hour is not a fixed amount. A salesperson's time during working hours in peak buying season is worth much more than the same individual's time after closing time in non-peak season. E-learning often enables the employee to shift learning to those non-peak hours.

The literature discusses a plethora of issues relating to e-learning other than costs. For instance, Filho (2005) claims that although content remains the most important factor in the success of e-learning programs, many companies have not figured out how to procure it effectively. Taylor (2002) concurs that no matter how sophisticated the technology is or how flashy the graphics and images are, it is the quality and relevance of the content to the business issue and learner objectives that coming out winning in the end. In the traditional instructor-led world, one of the ways training and development

programs differentiate is in the skill of the instructor. Everyone has experienced a time when weak material in the hands of a talented trainer still resulted in valuable knowledge transfer and skill acquisition. However, in the world of e-learning, weak content stands alone and therefore, is critical to the transference of knowledge.

Companies are still trying to find the right balance to make the e-learning experience engaging but not overwhelming. A chief concern during the next few years will be the viability of their e-learning vendors (Filho, Latham & Lundy, 2006). Since 2004, numerous vendors have been acquired, and major software vendors continue trying to enhance their capabilities. Simulation, gaming and interactivity can ramp up e-learning adoption and motivate its use. Academic and on-the-job research has shown that when students learn through experience, their understanding and retention is higher. Learning activities that engage students and activities that are highly immersive bring students closer to experiencing the activity or skill being taught.

The more advanced forms of e-learning are much more popular among larger firms and companies that are technology-savvy. According to Mullich (2004), at Fortune 400 firms, 73.6% of technology-delivered training comes through networked, online methods. Companies such as Canon, Cold Stone Creamery ice-cream store, and Cisco Systems have begun to use video games in their corporate training (Jana, 2006). Cold Stone Creamery ice-cream store's online training game teaches portion control and customer service in a cartoon-like simulation of a Cold Stone store. Players scoop cones against the clock and try to avoid serving too much ice cream. The company says more than 8,000 employees, or about 30% of the total, voluntarily downloaded the game in the first week. In another video game used by Canon employees, repairmen must drag and

drop parts into the right spot on the copier. As in the board game *Operation*, a light flashes and a buzzer sounds if the repairman gets it wrong. Workers who played the game showed a 5% to 8% improvement in their training scores compared with older training techniques such as manuals. Last year Cisco rolled out six new training games. Some of those games are designed to teach technicians how to build a computer network. In one Cisco game, players must put the network together on Mars. Including these interactive training tools, such as video games as part of an e-learning program, could prove to be a fairly simple way to decrease costs while at the same time engage employees to learn.

According to Broad (2005), the most obvious flaw of the evolving technology is the focus on the technology (the “e”) and not on the learning. It is this same misdirected focus that causes organizations to fail to capitalize on e-learning’s strengths to support transfer of learning to performance.

Aside from the corporate issues associated with e-learning, one cannot dismiss the personal attributes and self-efficacy associated with e-learning. Self-efficacy in this context describes an employee’s belief that he can be a successful e-learner. Mullich (2004) states that Sonesta Hotels, a chain of 25 properties stretching from Boston to Cairo, wants nothing to do with e-learning. The hospitality company tried to have employees learn customer-service techniques using self-paced computer modules, but found that, among other issues, the employees hated not being able to bounce ideas off one another during training.

Mungania (2003) conducted a study of e-learning barriers facing employees and found self-efficacy to be a significant predictor of barriers. Four key factors emerged as

significant predictors of e-learning barriers: (1) organization, (2) self-efficacy, (3) computer competence, and (4) computer training. High self-efficacy led to a perception of fewer e-learning barriers. Those who rated themselves as having no computer training and with low levels of computer skills were more likely to say they encountered barriers. Overall, successful e-learning demands social, cognitive, and behavioral skills. Accordingly, there are three major areas that were found to predict successful e-learning.

1. *E-learners' cognitive skills*: E-learners must have the prerequisite knowledge and skills necessary to participate in e-learning. Computer competency through training, and practice, and time management skills are essential.
2. *Environment*: Organizations must support e-learning by offering a supportive culture, incentives, models, resources, and fostering e-learning self-efficacy.
3. *Belief and behavior*: E-learners must have high e-learning self-efficacy and the appropriate behavioral skills such as taking responsibility for learning.

Although changes can be made to the organization, e-learning policy, design, and technologies, individual employees must take responsibility for their own learning. Frustrations are bound to occur regardless of other changes in the system if there is a lack of skills, low self-efficacy, and lack of responsibility. Furthermore, Broad (2005) contends that people tend to get so wrapped up in the technology that they forget that e-learning is still learning. As a medium for delivery and a process facilitator, electronically networked learning has tremendous potential to support transfer of vital skills in the workplace.

Summary

The literature prescribed emphasized the importance of measuring the effects of e-learning and provided a glimpse into problems that corporate trainers and employees may face. Far from being just another Internet fad, corporate e-learning is growing. It truly can transform the way organizations communicate, train their employees and increase productivity unlike nearly any other Web-based application. Training managers and executives understand that there must be a business strategy behind an e-learning program to ensure its impact.

The Contribution of the Study to the Field

The study has the potential to influence e-learning corporate training programs. E-learning metrics are in the early stages. Recommendations about how best to measure and evaluate learning and behavior and on transferring learning to behavior could have significant impact on the field. This research may provide information on measuring behavior long after the e-learning program has completed.

Chapter 3

Methodology

Introduction

The research methodology is the set of processes used to collect and analyze data (Leedy & Omrod, 2001). This chapter discusses the processes that were used for instrument development, sample selection, and collection and analysis of data. The goal was to produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies.

The methodology followed the Kirkpatrick Model, specifically Level 3. Many corporations, such as NCR, IBM and GE, use the Kirkpatrick framework to measure the success of e-learning (Beamish, Armistead, Watkinson, et al., 2002). NCR (Goldwasser, 2001) used post monthly training status reports to indicate that Kirkpatrick Level 3 was achieved. This level evaluation measures behavioral change on the job. It may include specific application of the special knowledge or skills learned in the training. It is measured after the training has been implemented in the work setting and may provide data that indicate the frequency and effectiveness of the on-the-job application (Phillips & Stone, 2003).

Three questions were answered in pursuit of the goal:

1. How must corporate strategies be presented so that they can guide the content and skills acquisition of e-learning?
2. How can the outcomes of training be measured to determine their effectiveness within the corporate strategies?

3. How can the evaluation process be used to increase tangible and intangible benefits to the organization?

Research Methods Employed

The extent to which changes in behavior and job performance have occurred as a result of the training event is measured by Kirkpatrick Level 3 evaluations. There are several data-collection methods often used for Level 3 evaluations including follow-up questionnaires and surveys, observations on the job, follow-up interviews and focus groups, work assignments, action planning, performance contracting, and follow-up sessions (Broad, 2005). A survey based on Phillips and Stone's (2003) Impact Questionnaire (see Appendix A) was developed in order to measure the value of e-learning and determine if it is linked to company goals.

The investigator developed a survey (see Appendix B) tailored for an e-learning class, *Information Security Awareness Training*. The Phillips and Stone's sample Level 3 evaluation survey was designed to be customized for a specific audience. Many questions from the example were tailored to fit the Information Security Awareness Training online course. Additional questions were added to the survey based on Broad's (2003) recommendation for analyzing Level 3 evaluations. These specific questions referred to actual workplace barriers to application of new learning observed by performers and use of support strategies by other stakeholders after the training.

Quantitative and Qualitative Methods

The approach for this dissertation used a combination of qualitative and quantitative components. The use of both methods provided more answers than the use of a single method (Leedy & Ormrod, 2001). With qualitative research, the researcher obtains the viewpoint of participants. Open-ended questions were used to allow participants to compose their responses. According to Fowler (2002), open-ended questions allow answers that can more closely describe the views of the respondents, and many respondents like the opportunity to answer some questions in their own words. These responses provided valuable insights in terms of the survey instrument, the training program and areas for improvement.

With quantitative research, the researcher collects numeric data from participants and analyzes the numbers using statistics to explain and predict the outcomes using statistical analysis and formal reporting (Leedy & Ormrod, 2001). Close-end questions also were analyzed with statistics. The quantitative questions on the survey fell into categories of interval scales. A Likert type scale was used with numbers 1 through 5. Some of the questions were assigned responses of “No Success” through “Completely Successful”. Other questions were assigned “No Opportunity to Apply” through “Significant Change.” There was an assumed equal distance between options.

Broad (2005) states that data for these evaluations are typically gathered three to six months after the intervention. The intention here was to develop a survey that examines the training impact over time. In addition, Broad states that on a Level 3 evaluation, learners may be asked to identify any actual workplace barriers that interfered with their ability to apply their new learning to performance on the job. Questions of this

nature were added to the survey. In general, the survey explored whether participants have modified their work behaviors based upon the learning experience.

The final survey consisted of eighteen questions. Question one asked if the participant was in a supervisory or management role. Question two was broken down into various sub-questions relating to the success in achieving various objectives learned in the online training. Question three asked if the participant implemented on-the-job actions plans as part of the training. Questions four through eight explored the level of improvement as influenced by participation in the online training. Questions nine through eleven asked if the company benefited from the training, if the training was a good investment and what has changed as a result of the training. Questions twelve through fifteen attempted to explore workplace barriers to applying the skills or behaviors learned in the training. Questions sixteen through eighteen sought out suggestions and comments for improving the online training and the survey. There were answers with the response of “Yes” or “No” in addition to open-ended questions that allowed the participants to a type free-form response.

Reliability Testing

The survey was tested for reliability and validity. Reliability is the degree to which a test consistently measures whatever it is measuring and refers to its consistency and stability over time (Phillips & Stone, 2003). Reliability should assure the researcher that the data gathered with a specific tool will remain relatively unchanged from one administration of the tool to another (Gay & Airasian, 2003). The investigator utilized the procedure recommended by Gay and Airasian to determine the test-retest reliability or

stability. The test was administered to a pilot group of eight people. After two weeks had passed, the same test was administered to the same group and the scores were correlated. The results of the two sets of data were nearly identical, and therefore, provided sufficient evidence that the test has good test-retest reliability.

Internal consistency reliability was also tested for one of the survey questions. Only Question 2 was written to describe a major construct and, therefore, was the only survey question that could be tested for internal consistency reliability. Question 2 consisted of six subquestions, which had a five-point Likert-type scale. Since a Likert scale seeks to measure a particular construct, its items must be identified as describing the same thing. Therefore, scales must have internal consistency in order to produce a reliable instrument (Gable & Wolf, 1993).

The calculation of internal consistency was assessed using the Cronbach Alpha Coefficient. Peterson (1994) stated that by either scholarly praise or volume of citation, Cronbach's alpha has effectively become the measure of choice for estimating the reliability of a multi-item scale. The value showing a number between zero and one represents the level of internal consistency among items in the scale – the closer the number is to one (the point where all variance is consistent), the more reliable is the instrument. According to Peterson, any Cronbach alpha value below .60 is unacceptable; the value of .70 indicates a low level of reliability, a value between .80 and .90 indicates a moderate to high level, and .90 and above indicates the highest level of reliability.

After the data were collated, the Microsoft Excel spreadsheet was imported into *Statistical Package for the Social Sciences* (SPSS) from SPSS Inc. The calculation of

Cronbach alpha was performed in the SPSS software. The internal consistency of the six subquestions comprising Question 2 was .903, representing a high level of reliability.

Validity Testing

Validity is concerned with the appropriateness of the interpretations made from test scores (Gay & Airasian, 2003) and ensures the tool measures what it is supposed to measure (Leedy & Ormrod, 2001). While there are several approaches to measure validity, the most frequently used for training programs is the content-validity approach (Philips & Stone, 2003). According to Gay and Airasian (2003) content validity is determined by expert judgment. Usually experts in the topic covered by the test are asked to assess its content validity. The panel examines the information about the objectives of the instrument, the content area, and the level of difficulty of the questions. Content validity can be evaluated by examining the plan and the procedures used in constructing the instrument (Creswell, 2005).

An expert panel reviewed the survey and provided opinions as to whether the process actually measures what is necessary or needed on the job for the particular topic. Four experts tested for reliability and validity: the utility's IM Training Coordinator, who has extensive experience in IT training, an employee of the IM Training Coordinator, the utility's IM Technical Supervisor under IM Cyber Security, who designed the *Information Security Awareness Training* e-learning course and an employee of the Technical Supervisor. These four members are subject matter experts because of their experience and job role.

The four experts responded to the draft survey commenting on the content and determining whether the questions covered the intent of the training. They ensured that the questions genuinely related to the topic of Information Security and to the online course. They also looked for unclear or ambiguous questions and to make further suggestions as to the content, number of questions, layout and design. As a result, the survey was refined. Some of the questions were removed and a couple of the questions were reworded. The survey was sent back to the experts for more feedback. The revised survey was then sent back a third time for final comments.

Construct validity was also tested. Gay and Airasian (2003) claim that construct validity is the most important form of validity because it asks the fundamental validity question: What is this test really measuring? Whereas the content-validity argument focused on the experts' judgments regarding the adequacy with which the test items reflected specified categories in the content universe, the construct validity argument focuses directly on response-data variation among items to ascertain evidence that the proposed content categories actually reflect constructs (Gable & Wolf, 1993).

Evidence of construct validity was gathered after the survey had been administered to the participants. An empirical analysis, factor analysis, was conducted in order to ascertain if there existed constructs that help explain the covariation among the items. Principal component analysis (PCA) is the most common form of factor analysis and is used to derive a small number of linear combinations (principal components) of a set of variables that retain as much of the information in the original variables as possible (Gable & Wolf, 1993).

The factor analysis was conducted on Question 2 that consisted of six subquestions. The purpose of the factor analysis was to determine if the instrument measured meaningful constructs. The extraction method used on SPSS was the PCA which was performed using the eigenvalue-greater-than-one criterion. The PCA showed that the six subquestions all loaded on one principal component, indicating that the subquestions as a group measure one construct. The first eigenvalue was 4.08, which is very high (see Table 2). All other eigenvalues were far less than 1; the second highest was 0.57. This first component explained 68% of the total variance.

Table 2.***Principal Components Analysis of the Six Subquestions of Question 2 (N = 142)***

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cum. %	Total	% of Variance	Cum. %
1	4.08	67.98	67.98	4.08	67.98	67.98
2	0.57	9.55	77.53			
3	0.50	8.35	85.88			
4	0.37	6.14	92.00			
5	0.31	5.17	97.19			
6	0.17	2.81	100.00			

Data Collection Procedures and Analysis

A pilot study is one in which the plan can be tried out on a small scale (Gay & Airasian, 2003). The purpose of the pilot study is to identify unanticipated problems or issues. In addition, it also allows the researcher to make any necessary changes before the actual administration of the survey takes place (Creswell, 2005). The study was pilot tested by eight IM employees who completed the questionnaire and indicated any ambiguous questions and noted the time on task. Within three days, all eight complied with the requests and provided valuable feedback. The final survey was revised based upon the suggestions.

Purposeful sampling was utilized. In qualitative research, the researcher intentionally selects individuals who have information that can help answer the research questions being studied. Creswell (2005) recommends that as a general rule of thumb,

the researcher should select as large a sample as possible. Given that all 700 Information Management employees completed the Information Security Awareness Training course, the target population for the survey was all IM employees. The survey was sent out after validity and reliability consistency had been determined, and approval had been granted for the proposal by the Institutional Review Board.

Permission was obtained from the Nova Southeastern University Institutional Review Board (IRB) to conduct surveys (Appendix C). The respondents were emailed a *cover letter* (Appendix D) that explained the purpose of the study. The communication was sent via company e-mail to request participation. The email provided a hyperlink to the website with the survey. The survey was housed electronically through Zoomerang (www.zoomerang.com). Although all IM employees were emailed the survey, some did not open the email and some chose not to respond. Further analysis of the response rate can be found in Chapter 4.

According to Creswell (2005), participation should always be voluntary and confidentiality should be assured. Zoomerang has an option to store the participant email address when they complete the survey. This option was turned off thereby not allowing the researcher to go back and tie an email address to a survey. Therefore, individual email addresses were not stored in the system and participants could not be identified. Given that emails from non-response surveys were not tracked, a reminder notice was not sent out. This was to reduce the risk of a participant completing a survey more than once.

Phillips and Stone's (2003) checklist for improving the response rate for questionnaires was considered. Some of the items on the checklist include keep the instrument simple and brief, estimate the time needed to complete the questionnaire,

make input anonymous, have the introduction letter signed by a top executive, consider incentives for completing and returning the forms and send a summary of results to the target audience.

Analysis Prior to Survey Creation

The data were gathered primarily through survey use. The survey instrument helped determine the alignment of training to corporate strategy. However, current literature determined that investigation of the company objectives had to be completed prior to the development of the survey. According to Kirkpatrick and Kirkpatrick (2005), once organizational strategy has been set and communicated, it is critical for training departments and corporate universities to align themselves closely with the strategy. The question is consistent with their recommendation to start with results and then determine with the line-of-business managers what needs to happen. This leads into Research Question 1, which explores how corporate strategies might be presented so that they can guide the content and skills acquisition of e-learning.

The balanced scorecard (BSC) is a popular tool that companies use to measure corporate strategy (Beasley, Chen, Karen & Wright, 2006; Cross, 2001; Kirkpatrick & Kirkpatrick, 2005; Pyzdek, 2004). Kirkpatrick and Kirkpatrick (2005) developed a step by step guide to depict how the BSC method can be used to determine the link between training and corporate strategies. The utility company uses a balanced scorecard to measure the link between corporate strategy and departmental IT strategy. The sole purpose of the instrument is to isolate key elements that leverage overall corporate strategy. Each line typically consists of the specific strategy, the BSC category, a

description of the measure, the actual measure, and the desired target. Therefore, in order to explore corporate strategy, an in-depth review of the current IT department's BSC was conducted to determine how it is linked to overall corporate strategy.

The IT department uses a monthly BSC called the *Information Management (IM) Scorecard Metrics* to measure performance against various targets. There are specific scorecards for key areas such as information security, financial, specific applications and operations. Measured components on the information security scorecard include percentage of workstations that are virus protected, percentage of servers that are virus protected and other security administration metrics.

There is also an overall IM Scorecard that measures department specific performance goals. Examples of specific metrics include the number of network outages, reduction of personal use workstations by 1% or more and percentage of email availability.

However, the measurement of information regarding the College of Information Management is done through the use of analytics rather than an IM Scorecard. The overall target for training is to measure the percentage of IM employees with 24 hours or greater of training reported as a graph on a monthly basis. There is an assumption that completing training is equivalent to mastery, however the measurement is solely based on the number of hours completed within the year. There is also a page that highlights the e-learning courses that have been completed.

The purpose of the review was to determine if any of the categories on the IT BSC aligned to training and development. For instance, a given measure might have corresponded to the strategic objective of *increased employee retention*. Although the

IM BSC links various targets to corporate strategy, there was not a clear link to training and development. In addition, there was not a category on the current BSC for learning and growth measures. Therefore, based on Kirkpatrick and Kirkpatrick's (2005) method of using a BSC to link training to corporate strategies, Chapter 5 makes recommendations as to how the IM BSC can depict corresponding measures for each of the strategic objectives.

Research Questions 2 and 3 explored the implementation of the training. The extent of transfer of skills and knowledge to performance in the work setting was measured by Kirkpatrick Level 3 evaluations as per Bersin (2002) and Broad (2005). Kirkpatrick and Kirkpatrick (2005) recommend working backward with the question, "What behaviors need to be put into practice to achieve the desired results?" Essentially, first it was important to analyze the corporate targets that need to be put in place and then determine tangible behaviors needed to reach each goal.

Format for Presenting Results

Chapter 4 presents the answers to each of the 18 survey questions. Zoomerang provides a summary of the data for the numerical questions and all of the responses to the open-ended questions. The numerical data from Zoomerang were transferred to an Excel spreadsheet to further compile and analyze the results and sort through the responses. Summaries are provided as well as the mean and mode for quantitative questions. In addition to written summary descriptions of the survey results, summary tables are also used for visual reinforcement. The open-ended responses were first interpreted, then

grouped into similar responses and put into categories, and finally, summarized. Since the responses were anonymous, some of the direct quotes are used.

Resources Used

The expert panel was a resource to give guidance for the survey and validate the content. The panel consisted of four experts in either the field of Information Security or the field of corporate online training.

Online software www.Zoomerang.com housed the survey and the results. Zoomerang provides extensive online survey services in addition to support. In addition, the site was used to compile responses as the surveys were taken. All participants had Internet access. Microsoft Excel was also used to compile and analyze the data collected for the study.

The investigator's employer provided the expert panel, utilization of the corporate email system to communicate with the target population, developed the online training course and provided input into the survey. Approval was obtained from the Human Resources Department and the Information Security director to administer the survey.

Summary

The purpose of the study was to produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies. The research question of how to actually align IT e-learning with corporate goals was analyzed through the balanced scorecard method. The remaining research questions were answered through a departmental survey.

The survey was administered to a department of Information Management

employees. The survey had both closed and open-ended questions and used both quantitative and qualitative research. The closed ended questions had answers from which the participants could choose. These responses corresponded with the values 1 through 5. Statistical analysis of the responses can be accomplished when pre-determined values are used.

The open-ended questions asked the participants various questions such as, *what were the barriers encountered that prevented you from using the skills obtained in the online training?* These open-ended questions were grouped into similar categories and summarized throughout Chapters 4 and 5.

Reliability was tested by a pilot group of eight people. The results of the tests were correlated and determined to have good test-retest reliability. An expert panel reviewed the survey for content-validity. The panel looked for unclear or ambiguous questions and made suggestions as to the content, number of questions, layout and design of the survey. Revisions were made based on feedback from the expert panel.

After the survey was given, the data were interpreted, categorized and summarized. The data are reported in both narrative and chart form.

Chapter 4

Results

The purpose of this study was to produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies. According to Phillips and Stone (2003), a significant problem that has plagued the training and development field for many years is a lack of transfer of what is learned by the participants from the training setting to the job setting. It is critical to ensure that learning occurs and that it is transferred to the job. A survey was conducted to measure the extent of transfer of skills and knowledge to performance in the work setting.

The data analysis discusses the survey return results using descriptive statistics including the sample size, mean, mode and standard deviation. According to Gay and Airasian (2003), when presenting the results of a questionnaire study, the response rate for each item should be given as well as the total sample size and the overall percentage of returns. This is because not all respondents will answer all questions. Each section of the survey will be summarized as well as the comments and suggestions made by the participants.

Findings and Analysis of Data

All Information Technology (IT) personnel in the utility company were required to take the Information Security Awareness Training online course. There was confirmation in October 2006 that 100% of the employees had completed the course. On March 22, 2007, about six months after everyone had completed the course, the survey

was sent out via email through the company's School of Information Management to all 700 IT personnel. The survey was left open until April 9, 2007.

There were 145 surveys completed. The survey was stored on the Zoomerang.com Web site. In addition to the number of surveys completed, the site also stored the amount of visits to the site, which was a total of 254. The number of surveys completed is not included in the 254.

There are a few possible reasons why 254 opened the survey but did not participate in the survey. The Information Management Security group, which is part of IT, was told not to take the survey as to not skew the results. They may have opened up the survey out of simple curiosity. The Chief Information Officer (CIO) sent the researcher an email stating that although he took a look at the survey, the questions did not apply to his everyday work and he did not want to skew the results. This may have also applied to other IT personnel who also thought they should not take the survey.

There are also many possible reasons why the remaining 300 out of 700 did not open the survey or complete the survey. Over the course of two weeks, people could have been on vacation, taken a leave of absence, been out on training or simply recognize that the email address was from the College of Information Management and deleted the email. In addition, some upper management have secretaries read their emails and it may not have ever been forwarded to them. Or it could have been that some people were simply too busy and did not have time to take the survey.

The response rate for the survey was 21% which was calculated by dividing the 145 completed surveys by the 700 distributed emails. However, the true response rate

may be a little bit higher given that some people (i.e., Information Management Security, CIO, etc.) should not have been included in the population.

The summarized data in the following sections are based on the answers to the 145 completed surveys. It should be noted that the participants were not forced to complete all questions in order to submit the survey. A few participants did not answer all questions, so there are a different number of responses for each question.

Survey Question 1: Supervisory or management role

Most of the participants were not in a supervisory or management role capacity; 27% stated that they were in a management role and 72% indicated that they were not (see Table 2).

Table 3. Supervisory or Managerial Role

Are you in a supervisory/managerial role?		
Yes	39	27%
No	102	72%
Total responses to this question	141	100%

Survey Question 2: Reviewing objectives from the online training

The intent of the second question was to determine the individuals' perception as to the degree of success in achieving certain objectives. Five objectives were chosen directly from the online training course objectives. Overall, participants felt that they were successful in understanding the objectives of the training course. Over 95% were successful in understanding company policies, the difference between strong and weak passwords and the dangers of computer viruses, worms and trojan horses. Over 85%

were successful in understanding the concepts of adware and spyware and data protection.

Recognizing instances of social engineering was one of the objectives in the training. Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information (Social Engineering, 2007). The term is typically applied to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim. In analyzing survey question 2, social engineering was found to be the weakest area where 18% had limited to no success understanding this objective (see Table 3).

Table 4. Objectives of the Information Security Awareness Training

Objectives of the Information Security Awareness Training										
1=No Success, 2=Very Little Success, 3=Limited Success, 4=Generally Successful, 5=Completely Successful										
		1	2	3	4	5	Total	Mean	Mode	Std. Dev.
2a	Have an overall understanding of company policies and that inadvertent or accidental violation of security policy will result in penalties	2	1	4	71	66	144	4.38	4	0.71
2b	Understand the difference between strong and weak passwords	2	0	3	28	112	145	4.71	5	0.64
2c	Realize ways that Viruses, Worms, and Trojan Horses can get loaded onto your computer without your knowledge	2	0	6	54	83	145	4.49	5	0.71
2d	Awareness of Adware, Spyware and Phishing and describe the dangers of each	3	3	11	55	73	145	4.32	5	0.87
2e	Define and recognize instances of social engineering and outline how to respond if you are the victim of an attack	4	1	21	57	61	144	4.18	5	0.91
2f	Describe Data Protection, identify customer and personal data, and summarize company data handling procedures	2	2	15	67	58	144	4.23	4	0.80

Survey Question 3: Implementation of on-the-job actions plans

The intent of this question was to determine if participants implemented on-the-job action plans as part of the training. According to Phillips and Stone (2003), the action plan is the most common type of follow-up assignment once a training course has been

completed. Action plans contain detailed steps to accomplish specific objectives related to the program. The action plan shows what is to be done, by whom, and the date by which the objectives should be accomplished.

All participants answered this question and 42% of the participants did implement on-the-job action plans (see Table 4). The researcher decided not to request participants to submit their action plans due to the anonymity of the survey.

Table 5. Implementation of On-the-job Action Plans

Did you implement on-the-job action plans as part of the Information Security Awareness Training?		
Yes	61	42%
No	84	58%
Total responses to this question	145	100%

Survey Questions 4 through 7: Level of improvement indicators

The next section of the survey focused on several areas covered in the training. Participants were to indicate their level of improvement during the last few months as influenced by their participation in the online training. Each separate question listed a few specific topics that were covered in the training.

Question number 4 reviewed company policies. Of the 145 participants who responded to the question about installing unapproved software, 30% did not have the opportunity to apply this policy and 32% stated that there was no change in their level of improvement. There were 12% who stated that they had a moderate change and 15% had a significant change. Those participants most likely were not aware of the policy.

In general, participants were clear before the training on the company policies. The most significant areas of improvement were the topics related to connecting to untrustworthy networks at 26% and using email for sending or receiving junk mail at

35%. The least area of improvement was the topic of coordinating the installation of a DSL, which is a Digital Subscriber Line that allows connection to the Internet, line or wireless access points through computer support. A total of 79% either had no opportunity to apply or showed no change in the level of improvement (see Table 5).

Table 6. Level of Improvement – Company Policies

Level of Improvement during the last few months - Company Policies										
1=No Opportunity to Apply, 2=No Change, 3=Some Change, 4=Moderate Change, 5=Significant Change										
		1	2	3	4	5	Total	Mean	Mode	Std. Dev.
4a	Installing unapproved software	43	46	18	17	21	145	2.5	2	1.40
4b	Connecting to untrustworthy networks	37	45	15	17	31	145	2.72	2	1.50
4c	Limiting personal use of company assets to appropriate use during approved times	15	53	31	20	26	145	2.92	2	1.28
4d	Using email for sending or receiving junk mail	20	56	18	21	30	145	2.9	2	1.38
4e	Coordinating the installation of DSL line or wireless access points through computer support	67	47	9	5	16	144	2	2	1.30

The intent of question number 5 was to evaluate the participants' understanding of password security and social engineering. The training focused on password security such as ensuring that users do not enable any software application or Web browser to *remember or save* passwords, not storing passwords in an obvious place such as posted on a monitor and the creation of complex passwords.

Most participants were knowledgeable on the subject of passwords. The largest level of improvement in this category was the awareness of the concept of shoulder surfing, which is a type of social engineering. Shoulder surfing is the use of direct observation techniques, such as looking over someone's shoulder, to get information. Over one half the participants, 53%, had some level of change in this category.

In the other areas there were also some acknowledged changes. The concept of not enabling any software application or web browser to *remember or save* a password had a 45% change. In the area of where to physically not store passwords there was a

37% change and the awareness of non-technical related issues such as impersonation of another employee there was a total 40% change (see Table 6).

Table 7. Level of Improvement – Passwords and Social Engineering

Level of Improvement during the last few months - Passwords and Social Engineering										
1=No Opportunity to Apply, 2=No Change, 3=Some Change, 4=Moderate Change, 5=Significant Change										
		1	2	3	4	5	Total	Mean	Mode	Std. Dev.
5a	Not enabling any software application or web browser to "remember to save" your password	19	60	22	17	26	144	2.80	2	1.33
5b	Not storing passwords in an obvious place such as posted on a monitor	17	74	12	10	31	144	2.75	2	1.37
5c	Awareness of non-technical related issues such as impersonation of another employee	34	53	20	11	26	144	2.60	2	1.40
5d	Awareness of the concept of shoulder surfing	20	48	30	16	30	144	2.92	2	1.36

The next question 6 explored participants' grasp of computer viruses, worms, adware and spyware. A computer virus or computer worm is a computer program that can copy itself and infect a computer without permission or knowledge of the user. Adware is software with advertising functions integrated into or bundled with a program. Finally, spyware is computer software that is installed surreptitiously on a computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent. Spyware programs can collect various types of personal information, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, or diverting advertising revenue to a third party.

In general, most participants were aware of these concepts. The most significant change, 25%, was the act of deleting unsolicited emails with attachments. About 49% of the participants made at least some change in both recognizing if a computer's performance is unexpectedly slow and not clicking on links in embedded in emails. The area that showed the least level of change corresponded to the awareness of the antivirus

icon error message where 61% of the participants either had no opportunity to apply or had no change (see Table 7).

Table 8. Level of Improvement – Viruses, Worms, Adware and Spyware

Level of Improvement during the last few months - Viruses, Worms, Adware and Spyware										
1=No Opportunity to Apply, 2=No Change, 3=Some Change, 4=Moderate Change, 5=Significant Change										
		1	2	3	4	5	Total	Mean	Mode	Std. Dev.
6a	If the antivirus icon has an error, call the help desk	49	40	19	16	21	145	2.45	1	1.42
6b	Send hoax emails to the "Spam email" address and then delete it	29	48	21	19	28	145	2.79	2	1.42
6c	Recognize Spyware such as pop-up ads	27	52	24	20	21	144	2.69	2	1.32
6d	Recognize if a computer's performance is unexpectedly slow	25	49	31	17	23	145	2.75	2	1.32
6e	Delete emails that have attachments that you did not request	24	54	18	13	36	145	2.88	2	1.46
6f	Do not click on links embedded in emails	16	57	25	17	29	144	2.9	2	1.33

Question number 7 explored the sensitive issue of data protection or data privacy. Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data. Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues (Data Privacy, 2007).

There were about 65% who indicated that they had at least some increased awareness that the company is an attractive target for identity theft fraudsters, who are those people that exploit means of identification for an unlawful purpose. Only 35% either had no opportunity to apply or had no change meaning that they were already aware of this potential threat.

Almost half, about 42% already understood that destruction of confidential records must be done with some form of disintegration such as shredding. However, 22% made a significant change in that area.

There were 58% that made at least some change in understanding the company is responsible for protecting data such as social security numbers, bank information, date of birth and driver license information (see Table 8 for additional statistics).

Table 9. Level of Improvement – Data Protection

Level of Improvement during the last few months - Data Protection										
1=No Opportunity to Apply, 2=No Change, 3=Some Change, 4=Moderate Change, 5=Significant Change										
		1	2	3	4	5	Total	Mean	Mode	Std. Dev.
7a	Increased awareness that the company is an attractive target for identity theft fraudsters	11	38	37	24	34	144	3.22	2	1.28
7b	Destruction of confidential records must be done with some form of disintegration such as shredding	14	47	26	26	32	145	3.1	2	1.33
7c	Understand the company is responsible for protecting data such as social security numbers, bank information, date of birth and driver license information	11	50	22	18	43	144	3.22	2	1.39

Survey Questions 8 through 10: Open-ended, free-form questions

In the next section of the survey the participants were able to reflect openly on their own post-training knowledge. The questions were open-ended, free-form and optional. According to Gay and Airasian (2003), an unstructured item format, in which the responder has complete freedom of response, permits greater depth of response and insight into the reasons for responses. Furthermore, for certain topics or purposes unstructured items may be necessary and some questionnaires do contain both structured and unstructured items.

Question number 8 asked the participants to list the three behaviors or skills from the above list (Questions 4 – 7) that the participant has been made most aware of as a result of the training. Because the format was free-form some participants did not list a specific behavior. For instance, some participants stated as their top three behaviors: passwords, viruses, and company policies. However, the researcher was asking for

specific behaviors such as awareness of shoulder surfing. If this survey is sent out again to another population, a drop down box would be provided so that the participant could pick the specific behavior rather than allow a free-form text.

Table 9 displays a breakdown of the areas covered in the training. There were a total of 242 responses from 100 different participants. This is because some participants only listed one or two behaviors. The largest area of awareness at 33% was passwords and social engineering. Within this area, the most frequent response was the behavior of creating strong and complex passwords. The least affected area was company policies at 12%. This is a solid indication that most employees are cognizant of the company policies around information security.

There were four participants who stated that they were aware of all the skills prior to the training. There were two responses that were unknown because they could not be placed in a stated area. There was one comment that was not used in the statistics which stated that the training was a, “general reinforcement of good information security practices.” And the final comment that was excluded from analysis stated, “What list?” (see Appendix E for a complete breakdown of responses to question #8).

Table 10. Skills Most Aware of as a Result of the Training

The 3 behaviors/skills that the participants have been made most aware as a result of the training		
	Total	%
Company Policies	30	12%
Passwords and Social Engineering	80	33%
Viruses, Worms, Adware and Spyware	75	31%
Data Protection	51	21%
Unknown Responses	2	1%
Participants already aware before the training	4	2%
Total Responses	242	100%

In question number 9 the participants were asked how the company has benefited from participation in the training. The participants were asked to identify specific business improvements believed to be linked to participation in the training. This question was optional, free-form text and received 95 responses.

About 5 of the total 95 responses either stated *N/A*, *none* or just the word *yes*. However, the remainder of the responses listed specific business improvements. For instance one participant stated that the email system is available 100% of the time. A few participants stated the increase in the general awareness of tactics used by criminals to obtain confidential information. Many listed that their computer is virus free and the network has not been infected. One participant stated that they will train business unit customers about the dangers of computer viruses.

The most significant finding was that many of the participants felt that this training was a beneficial reinforcement and refresher of security practices. Many of the participants also stated that this training would be helpful for less technical employees. And a few had statements related to the Internet such as, "I am a smarter Internet user" and "will limit Internet use" (see Appendix F for all of the responses to this question).

In question number 10, the participants were asked what has changed about their work as a result of the participation in the training. This was another optional, free-form question that received 104 responses. Interestingly, there was at least one response for each and every content area covered in the training. Approximately 10% of the responses stated that nothing has changed because of the training. A few of those 10% stated that nothing has changed because they were already aware of these security issues.

Many of the responses in this question referred to the area of password protection. For instance some participants stated that they no longer allow the system to save their passwords and that they make a conscious effort to create stronger passwords. Also, a few people stated that they now lock their computer before leaving their desk. One person stated specifically, “workstation is no longer left active when not at my desk even if for a minute.”

A few discussed the importance of paying closer attention to emails, potential computer viruses and using the shredder for sensitive data. Overall, there were many who stated in some form that they are now overall more cautious since this training has reinforced topics that are used in their daily jobs (see Appendix G for a complete list of the responses).

Survey Question 11: Training as an investment to the company

Participants were asked if they thought the Information Security Awareness Training represented a good investment for the company. A total of 94% stated that it was a good investment and only 6% stated that it was not a good investment (see Table 10).

Table 11. Training as an Investment for the Company

Do you think the Information Security Awareness Training represented a good investment for the company?		
Yes	133	94%
No	9	6%
Total responses to this question	142	100%

Survey Question 12: Barriers encountered in trying to apply the new training skills

The intent of question number 12 was to learn if the participants encountered any barriers that may have prevented them from using the skills or behaviors gained in the Information Security Awareness Training. The participants chose their response from a list of 4 and were also able to type a free-form response into the *Other* box. Participants were asked to check all responses that apply to the questions and there were 97 total responses. Some people checked off more than one response which is why the total is over 100% (see Table 11).

There were 26% who stated that they had no opportunity to use the skills learned in the training. About 15% stated that they have not had enough time to apply the skills. However, the researcher launched the survey 6 months after the last training class was taken. Another 2 percent stated that their work environment does not require them to use the skills and 3 percent stated that the material does not apply to their job situation.

There were 54 responses that were typed in. Of the 54 typed in responses, about one-half or 52% of the participants typed in that there were no barriers. Obviously, if this survey is used again, *No barriers* should be an option on the form. There were comments such as: “Good practices are not embedded into our culture”, “I am able or required to apply all techniques”, and “Our SPAM filter could use more improvement.” A couple of people noted that it is too hard to remember multiple *smart* passwords (see Appendix H for detailed responses to question 12).

Table 12. Barriers Preventing Participant From Using the Skills

What barriers if any have you encountered that have prevented you from using the skills/behaviors gained in the Information Security Awareness Training? Check all that apply.		
I have had no opportunity to use the skills	24	26%
I have not had enough time to apply the skills	14	15%
My work environment does not require me to use these skills/behaviors	2	2%
This material does not apply to my job situation	3	3%
Other, please specify	54	58%
Total Responses	97	104%

Survey Question 13: Additional support that management could provide

Question 13 asked participants what additional support could be provided by management that would influence their ability to apply the skills and knowledge learned from the training. The questions were open-ended with a total of 64 responses (Appendix I). About 41% of the participants stated either, “none”, “n/a”, or “no ideas at the moment.” There was one comment, “don’t threaten employees for accidentally violating security policy resulting in penalties.” Another person commented that it might be helpful to provide examples of real world situations of data security breaches.

The responses can be summed up into the following top 10 areas for recommendation to management:

1. Communicate the Information Security Training course to all business units
2. Provide better SPAM (unsolicited, bulk email) filter control
3. Enforce the security policies via email or internal Web sites
4. Provide follow-up training and discussion this includes high level review in staff meetings and periodically bringing up key points of the training

5. Implement Single Sign-on thereby eliminating multiple passwords for different systems
6. Keep current on the latest Virus/Spyware software
7. Force newly hired employees to take the training class
8. Provide more training, tips and tricks for Data Security
9. Provide constant reminders about the dangers of emails and other data sources from outside the company
10. Request customer business units to take the refresher test each year

Survey Question 14: Follow-up supervisor discussions

Question 14 was a two-part question. The first question asked if their supervisor discussed the training after completion of the course. Of the 137 responses (Appendix J), 21% did have follow-up discussions and 79% did not have follow-up discussions (see Table 12).

The second part of this question stated that if the supervisor had a follow-up discussion, indicate one or two points that were discussed. One of the participants listed both data and password protection and the importance of not surfing the Web so that spyware will not penetrate into the system. Others stated company policies while another person stated the importance of Internet use should be for company business only. The most significant finding was that many of the participants who answered *yes* stated that the training was discussed in a staff meeting.

Table 13. Supervisor Follow-Up Discussions

Did your supervisor discuss the training with you after you completed the program?		
Yes	29	21%
No	108	79%
Total responses to this question	137	100%

Survey Question 15: Other support received after the training

This question asked if other support or encouragement was received for applying the training. Of the total 134 responses, 29% stated that there was other support and 71% stated that there was not other support (see Table 13). The researcher should have included an open-ended question for the 39 participants who stated that there was additional support to actually list out the items.

Table 14. Additional Support

Was other support or encouragement received for applying the training?		
Yes	39	29%
No	95	71%
Total responses to this question	134	100%

Survey Question 16: Topics that were not covered

Question 16 asked what specific topics of interest were not covered in the training. There were a total of 12 responses (Appendix K) which were as follows:

1. Best practices for personal data file protection
2. Employee recourse
3. How to better use Internet options for security purposes
4. How to prevent SPAM email

5. Identity theft repair
6. Request for a reference/hardcopy booklet
7. Procedure for getting outside vendors network access while working within the company network
8. Security around the Blackberry
9. Setting up firewalls for home computers
10. Use of *thumb* drives
11. Use of external memory media from home for working at home
12. Destruction of media such as CD, DVD cell phones and Blackberries

Survey Question 17: Suggestions for improving the training

Question 17 asked for specific suggestions on improving the training. There were 47 total responses (Appendix L) to this question although 29 participants actually typed in “n/a” or “none.” The top 8 suggestions were as follows:

1. Provide more information about protecting the home computer
2. Do not threaten employees
3. Provide friendly reminders
4. Review Internet options for security purposes
5. Repeat the training every 6 months; another said to repeat it annually
6. Include more realistic discussions of real world security breaches
7. Make the training more technical for the IT group
8. Include contractors to take the training class

Survey Question 18: Other comments

Question 18 asked for other comments and there were 15 responses (Appendix M). One participant was concerned about the cleaning crew and wrote, “Facilities management should consider the people who come in to clean especially behind the locked doors. To me this is an issue with laptop theft.”

Seven of the responses related directly to the survey. For example, one participant stated that in questions 4 through 7 there should have been a response, “Already employing concepts.” Another person stated that the survey should have been sent out sooner because they remember taking the class but do not remember the details of the content.

Finally, there were some positive comments about the training in general. Three participants stated that it was good training and glad that it applied to work and home habits. Another person simply stated, “Great training.”

Summary

This chapter has presented the findings of research collected by a Web-based survey. Findings about the Information Security Awareness Training course were gathered and analyzed. The survey was administered approximately six months after the completion of the course in order to give participants the opportunity to apply the new knowledge.

The focus of the survey pertained to analyzing the level of success in understanding the key objectives from the online training and the level of improvement as influenced by the training. As a result of the training, participants were mostly made

aware of the importance of complex passwords and social engineering behavior. The area following closely behind was the obscure and often ignored concepts of viruses, worms, adware and Spyware. Overall, participants felt that the training represented a good investment for the company and offered valuable feedback as to the additional support that management could provide to further influence the ability to apply the skills and knowledge learned from the training. In addition, participants offered topics that could be added to the training and suggestions for improving the training.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Introduction

Chapter 5 begins with the conclusions drawn from the results of the study using the research questions as a basis. This is followed by a review of the implications and recommendations to the research community for future research. The recommendations section focuses on the main purpose of this study which was to produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies. The chapter closes with a complete summary of the entire dissertation.

Conclusions

Three research questions formed the foundation for the goal of this dissertation which was to produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies. The questions along with a discussion of the answers to be drawn from the results of the study follow.

- **Research Question 1: How must corporate strategies be presented so that they can guide the content and skills acquisition of e-learning?**

According to Kirkpatrick and Kirkpatrick (2005), once organizational strategy has been set and communicated, it is critical for training departments and corporate universities to align themselves closely with the strategy. The question is consistent with

their recommendation to start with results and then determine with the line-of-business managers what needs to happen.

The balanced scorecard (BSC) is a popular tool that companies use to measure corporate strategy (Beasley, Chen, Karen & Wright, 2006; Cross, 2001; Kirkpatrick & Kirkpatrick, 2005; Pyzdek, 2004). Kirkpatrick and Kirkpatrick (2005) developed a step by step guide to depict how the BSC method can be used to determine the link between training and corporate strategies. The utility company uses a balanced scorecard to measure the link between corporate strategy and departmental IT strategy. The sole purpose of the instrument is to isolate key elements that leverage overall corporate strategy. Each line typically consists of the specific strategy, the BSC category, a description of the measure, the actual measure, and the desired target. Therefore, the first step was an in-depth review of the current IT department's BSC to determine how it is linked to overall corporate strategy.

The IT department uses a monthly BSC called the *Information Management (IM) Scorecard Metrics* to measure performance against various targets. There are specific scorecards for key areas such as information security, financial, specific applications and operations. Measured components on the information security scorecard include percentage of workstations that are virus protected, percentage of servers that are virus protected and other security administration metrics.

There is also an overall IM Scorecard that measures specific performance goals. Examples of specific metrics include the number of network outages, reduction of personal use workstations by 1% or more and percentage of email availability.

However, the measurement of information regarding the College of IM is done through the use of analytics rather than an IM Scorecard. The overall target for training is to measure the percentage of IM employees with 24 hours or greater of training reported as a graph on a monthly basis. There is also a page that highlights the e-learning courses that have been completed.

The purpose of the review was to determine if any of the categories on the IT BSC aligned to training and development. For instance, a given measure might have corresponded to the strategic objective of *increased employee retention*. Although the IM BSC links various targets to corporate strategy, there is not a clear link to training and development. In addition, there is not a category on the current BSC for learning and growth measures. Recommendations are made below as to how the IM BSC can depict corresponding measures for each of the strategic objectives.

IM should build a learning and growth category on the current BSC. These measures will track foundational initiatives that must be in place for the company to perform in an effective manner. Aligning measurement methods with strategy will improve focus. The building of the proposed learning and growth category is based on Kirkpatrick and Kirkpatrick's (2005) method of using a BSC to link training to corporate strategies.

The major steps for building the scorecard are:

1. Develop strategy maps that depict overall organizational strategic themes.
2. Develop corresponding strategic objectives from the strategic themes.
3. Develop corresponding measures for each of the strategic objectives.

Using the example from the dissertation as an area for measurement is *Increase awareness of information security*. Table 14 illustrates this theme.

Table 15. Creating a Strategic Theme

Strategic Theme	Strategic Objective	BSC Measure
Increase awareness of Information Security	Decrease employee lay offs due to inappropriate computer usage	Number of employees laid off due to inappropriate computer activity
	Increase computer down time due to viruses in the network	Monitor computer down time and slow performance
	Decrease calls to the Help desk for questions such as SPAM and password changes	Percentage of HELP desk calls relating to Information Security

Referring to Table 14, there is one strategic theme that generates three different objectives. If these objectives are executed properly they will lead to improvement. The corresponding three measures allow the company to know how well this strategy is going, culminating in the obvious production measure of increasing awareness of information security.

- **Research Question 2: How can the outcomes of training be measured to determine their effectiveness within the corporate strategies?**

It is important that there should be a clear link between the business problem and the learning objectives. Mayberry (2007) emphasizes that the course and learning objectives should be designed with the Level 3 assessment in mind. This means that the training should state the learning outcomes in observable measurable terms. This will facilitate in collecting and analyzing Level 3 performance data.

In addition to the Level 3 survey, data collection can also be done through a combination of direct and indirect observations. Indirect observation is often in the form of data that results from the desired behavior or performance. For example, the number of employees laid off during the month of May for security breaches might be an indirect observation.

Direct observation involves witnessing the learner's behavior in an actual setting. For example, a manager may walk around the halls during lunch time to ensure people have their computers locked (i.e., password needed to re-enter). Another valuable observation might be to sample some of the network passwords. It would be curious to track whether or not the complexity of the passwords has changed over time. Many noted in the survey that this was the objective that they were most made aware of during the online training.

In terms of data collection, there are also challenges pertaining to opportunities to demonstrate the newly learned skills. Some survey respondents noted that they have not had the opportunity to apply the new skills and others noted that the training was so long ago they could not remember. Consequently, it may be necessary to move the Level 3 assessment to a different time period. In addition, if too much time passes between training and application of skills, it may be time to conduct a refresher course. Quick reference materials may also be required.

Overall, opportunities to demonstrate the skill, behavior or knowledge should be identified before the training occurs. The training should occur no more than one month before the application. It is important to note that to be successful with any behavioral change, there should be meaningful consequences linked to the behavior demonstrated.

These consequences should be shared with the learner prior to taking the training, of course in a non-threatening way. One of the comments from the survey stated that the respondent *did not appreciate being threatened*. It is important that learners understand the consequence to the company because without consequences, behavior will not change.

- **Research Question 3: How can the evaluation process be used to increase tangible and intangible benefits to the organization?**

Intangibles are factors that cannot easily be directly linked to results. Tangible benefits are more obvious and can sometimes be linked to monetary values. In accordance with Phillips and Stone (2003), Table 15 has been constructed to present the most common intangible variables. They are positive results that either cannot be converted to monetary values or would involve too much time or expense in the conversion to be worth the effort. However, even though any of the intangible benefits may not be converted in one evaluation study, they may be converted in another study or in another organization. In some situations, intangible effects on teamwork, job satisfaction, communication, and customer satisfaction are as important as monetary measures. Another challenge to organizations is to leverage the intangibles into tangible behaviors and results.

There are many potential intangible benefits to the Information Security Awareness Training course. For example, by allowing employees to be cognizant of how to prevent computer viruses, the hope is that this behavior will lead to decreased computer down time. Ultimately, decreased computer down times should lead to fewer

customer complaints and fewer employee complaints. Depending on the size of the company and the impact to its customers, this could even lead to an enhanced community image.

Table 16. Common Intangible Benefits

Increased job satisfaction	Decreased customer dissatisfaction	Increased organizational commitment
Enhanced community image	Improved work climate	Enhanced investor image
Fewer employee complaints	Fewer customer complaints	Fewer employee grievances
Faster customer response time	Reduction of employee stress	Increased customer loyalty
Increased employee tenure	Improved teamwork	Reduced employee lateness
Increased cooperation	Reduced absenteeism	Reduction in conflict
Improved decisiveness	Reduced employee turnover	Increased innovation
Improved communication	Increased customer satisfaction	

Adapted from "How to Measure Training Results," by J. J. Phillips and R. D. Stone, 2003, p. 224.

The evaluation process can be used to increase tangible and intangible benefits to the company. It is important to note that a challenge to organizations should be to leverage the intangibles into tangible behaviors and results. During the creation of a level 3 evaluation, key stakeholders should begin to question how behavior influences outcomes. For instance, determining what to do with SPAM email is a constant battle with employees. Many survey participants stated that they are now aware that SPAM email should not be opened and instead forwarded to a special email address. If a value can be placed on employee email decisiveness (potential cost to the company of opening a SPAM email *times* the number of emails per month sent to the SPAM email address = cost to the organization) then there will now be a tangible value in management terms.

Survey participants should be asked to identify intangibles. After all, it is their performance that is to be influenced. The participants should be able to explain how things change for them in the organization as they implement the new skills. In addition, managers often have a broader view of the work setting and can see the overall behavioral changes and how they impact important intangible measures.

Often during data collection intangible data can be collected from stakeholders. There may not always be a plan to collect intangible data, and it may not be anticipated in the initial planning. However, intangible data may surface on a feedback form, during an interview, or during a focus group activity. When questions are asked about improvements influenced by the training, participants may provide several intangible measures for which there are no plans to assign a value. For example, some survey participants claimed that they have an overall *increased awareness* of information security issues. This increased awareness can be seen as an intangible benefit to the company in addition to the benefit of their own home and personal computer security.

Limitations of the Study

Limitations may place restrictions on the findings of the study. Although a number of conclusions have been drawn as a result of this study, it is important to review some of the limitations against which these conclusions should be judged. First, this was a purposeful sample and the results should not necessarily be generalized. The participants came from only one organization. Second, although the sample size of 145 resulted in acceptable statistics, a larger sample size may produce different and statistically better results. Third, given that the participants were technically inclined,

they are more computer savvy than what a different population would represent. A less computer literate population may have focused more on the delivery of the training class thereby potentially producing different results.

There are a couple of conditions that are outside the control of the researcher. First, all participants have unique values and beliefs that influence their perceptions and, therefore, their survey responses. Second, although critical to a Level 3 evaluation, the survey was given 6 months after the online training was completed. The last few questions on the survey, “*What specific topics were not covered that you felt should be?*”, “*What specific suggestions do you have for improving this training?*”, and “*Other comments*”, may have been better answered immediately after the training.

Implications

There are important implications for the people involved in developing or rolling out a business related online training course. Discussions around the questions below should take place before the implementation of the training. These questions should have clear answers in order to determine if the training class was effective or if it should even be executed:

1. Is there a clear linkage to a business problem or organization goal?
2. Has the current learner capabilities and the desired levels of performance upon completion of the learning materials been communicated?
3. Have the key stakeholders been involved in defining the goals of the training?

For instance, if the key stakeholders lack buy-in or are not interested then maybe there is no need for the training.

4. Are there immediate opportunities to demonstrate the new skill, behavior or knowledge?
5. Are there negative and or positive consequences for behavioral changes?

Recommendations

The recommendations based on the results of this study fall into three areas. First are the recommendations to improve the Information Security Awareness Training Impact Questionnaire survey instrument. Second are the recommendations for practice. Falling under this area is a discussion of the main purpose of this study which was to produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies. And third are recommendations for future research.

Recommendations for the Information Security Questionnaire Survey Instrument

The next version of the Information Security Awareness Training Impact Questionnaire survey instrument should have the following revisions to improve the quality of the data collected.

1. Section 2 requested the respondents to indicate their degree of success in achieving various objectives. There were five pre-defined answers ranging from *no success to completely successful*. However, there should have been a sixth opportunity for the respondent to check off *already knew this information before the training*. Given that the participants were technically savvy, some of them

- already knew about such terms as computer viruses and worms before coming into the training.
2. Question 3 asked simply *yes* or *no* if the participant implemented in on-the-job action plans as part of the training. Given that a high 42% responded *yes*, a part 2 free form text question should be added to ask, *Please list specific examples as to the action plan and how it was implemented in your department.* As an alternative to the part 2 above, another question could have stated, *If you answered "Yes", please rate the extent to which you were able to carry out your plan on the job: Fully, very much, very little or not at all.*
 3. Sections 4 through 7 asked the participants to indicate their level of improvement during the last few months as influenced by their participation in the training. There were five responses ranging from *no opportunity to apply* to *significant change*. One of the responses was simply *no change*. Respondents were not all clear if no change meant that they were already performing these activities, such as installing unapproved software, before the training. There needs to be a clarification statement that explains *no change* to mean that the participant was aware and already performing these activities before the training.
 4. Question 12 asked, *What barriers, if any, have you encountered that have prevented you from using the skills/behaviors gained in the training?* In addition to the pre-defined answers, the following responses need to be added: (1) No barriers, and (2) Already aware of all information and following processes before the training was implemented. A part B question could have asked, *Were any of the barriers then removed? How and by whom? Please be as specific as*

possible. Knowing that these items are being asked could potentially motivate stakeholders to act promptly to remove barriers if they occur.

Recommendations for Practice

The main purpose of this study was to produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies. Each training program should be required to address specific performance deficiencies, and what is needed to achieve performance improvement. The success and importance of training should not be measured by the skills and competencies that are being developed, but by how well the training resolves specific on-the-job *problems*.

Table 14 depicts an overall *strategic theme* as an objective of the training course. However this high-level theme should be further broken down into sub-categories. Using the Information Security Training class as an example, a valid sub-theme could be password and social engineering rules. Table 16 depicts the objectives of the *password and social engineering rules* sub-theme, which was one of the critical lessons in the training course.

Table 17. Creating a Strategic Sub-Theme

Strategic Theme	Strategic Objective	BSC Measure
Password and Social Engineering rules	Encourage employees to create complex passwords	Instances of failed password attempts
	Educate employees about the various methods of social engineering	Instances of social engineering (attempted and failed)
	Decrease calls to the Help desk for password changes	Percentage of HELP desk calls relating to password changes

Referring to the second strategic objective in Table 16, social engineering is a technique used to trick people into divulging confidential information or taking unauthorized actions. In most cases, the attacker does not come face-to-face with the victim since contact is online or over the telephone. Among the more common techniques are *phishing* and *pretexting*. *Pretexting*, usually done on the telephone, uses an invented scenario (the pretext) to trick the victim. *Phishing* is the use of emails appearing to come from a legitimate business, i.e., bank or credit card companies, to elicit personal information such as credit card or social security numbers. These scams can be quite creative, appear convincing and can fool the unsuspecting and unaware.

The utility company referred to in this study has received attacks of this nature both online and over the telephone. Recently, someone falsely claimed to represent one of the company's board members and attempted to obtain information about a regulatory compliance program. Given that the utility company is a part of this nation's critical infrastructure and for reasons of operational security, employees and contractors need to be educated not to provide any non-public information to anyone unless the caller has an authorized need to know. Telephone calls requesting non-public or personal information that appears suspicious should be tracked as an example of a measure on the BSC.

Through the research of the literature and results of the study various issues, barriers, successes, evocations and goals are recommended:

1. Ensure that the online training is aligned with organizational goals. Table 17 offers guidelines on maximizing the impact of training.

Table 18. Aligning Training with Organization Goals

Ensure the online training is aligned with organizational goals Action item	Comments
1. Define and prioritize organization's mission and goals	
2. Identify tasks needed to achieve the goals	Tasks needed to achieve these goals should in-turn be identified, stated in measurable terms and prioritized
3. Assign tasks to various groups/jobs	Who needs to perform tasks needed to achieve the stated performance goals?
4. Determine which tasks require training	The attributes of each task (i.e., level of difficulty, level of importance, etc.) are further analyzed to determine if training is needed and the criterion performance level for this training
5. Prioritize the knowledge, skills and attitudes needed to perform tasks that require training	
6. Identify the knowledge and skill gaps	Existing and potential gaps may be revealed by comparing the knowledge, skills and attitudes needed by each group to achieve the desired level of performance, with the current knowledge, skills and attitudes of the group
7. Identify implementaiton issues	The feasibility of plausible training solutions should be assessed by examining the availability of funding and resources, compatibility with existing programs, and any organizational attitudes towards the proposed training solutions
8. Prioritize activities and prepare a plan of action	

Adapted from "Maximize training impact by aligning learning with business goals," by J. Bahlis, 2006, www.bnhexpersoft.com/english/resources/whitepaper.htm.

2. Develop an overall strategic theme further breaking this down into relevant strategic sub-themes (see Table 16).
3. By utilizing the BCS methodology, ensure these corporate strategies are presented in a way that they can guide the content and skills acquisition of e-learning. Most corporate trainers are aware that e-learning can provide just-in-time access to training material whenever needed, reduce travel costs and time required to complete training. Table 18 offers recommendations once it has been determined that online learning will be the method of delivery.

Table 19. Presenting Corporate Strategies for E-learning Format

Ensure these corporate strategies are presented in a way that they can guide the content and skills acquisition of e-learning Action item	Comments
1. Divide the online training into modules or sub-themes	Modules should be divided into prerequisites, underlying theory (if applicable), objectives
2. All training objectives within a module should have similar characteristics	
3. All training objectives should have real life examples and hands-on exercises	The learner needs to relate the objective to a real life situation. This can most easily be done through audio or video.

4. With Kirkpatrick's Level 3 methodology in mind, create a survey instrument based on the objectives from the strategic sub-themes. At first, the instrument may be a continual work-in-progress. If the survey instrument is broken down by strategic sub-themes it should become quite obvious if there were improvements as a result of the training. Analyzing the collected data may depict that there was not as much as a performance gap as previously thought in certain areas.

General recommendations also emerged as a result of this study. A compilation of the literature in addition to comments and inferences from survey recipients describe recommendations that will facilitate the successful transfer of learning to behavior.

1. Offer merit awards. Managers tend to pay rewards for reaching a goal (i.e., greatest call volume, referrals, number of closed tickets, etc). However, awards should also be offered for exhibition of the appropriate behaviors that lead to achieving the desired outcomes. Therefore, importance should be placed on behaviors and how employees do their jobs rather than only the end-result.

2. Dedicate time for workplace e-learning. It is important that there be dedicated time for workplace e-learning which should be a part of the working schedule. The delivery method is immaterial if the potential learner cannot commit the time necessary for the training class. Expecting employees to squeeze training in between other assignments is an expectation that is doomed to failure. Online training should be scheduled into the working day the same as a classroom training class would be scheduled in the working day.
3. Make sure employees get a chance to use immediately what they have learned. Managers should help trainees apply principles and concepts to their unique situations. An environment that does not support new behaviors drives people back to old ways of working.
4. Take care that managers observe and reinforce correct behaviors. Especially with online learning, managers should meet with employees and discuss expectations.
5. Ensure upper management understands that new behaviors and subsequent success takes time to build. These new behaviors should not be expected to depict changes for at least six months after the training.
6. Ask senior managers to call or visit top performers to recognize them.
7. Deliver information in small increments over time by splitting the course into smaller parts to allow time for on-the-job application.
8. Share the benefits of any new expectations.
9. If applicable, use group implementation to create mutual support.
10. If applicable, use learning assignments between training sessions.

11. Engage high performers in the creation of online learning courses as well as post-training evaluations.
12. Conduct post-training evaluations late enough that employees have had time to internalize the concepts which should result in lasting changes. Overall, a six month period is recommended to give people time to think about the concepts, practice the principles, receive feedback, make adjustments, and overcome stumbling blocks.
13. Once training has been completed, the learner should use job aids and network with other learners for support.

Recommendations for Future Studies

Based on the conclusions, findings, and limitations of this study, there are several recommendations for future research. Future researchers may wish to consider conducting a survey to a non-IT group. Given that these group of individuals are very familiar with the technical aspects of e-learning, the survey may produce different results on a group that have an average history of computer usage or even may not have experienced e-learning previously. Researchers who wish to replicate this study should consider using a larger number of respondents to validate the results of the study.

In addition to evaluating e-learning at Level 3, a future researcher might consider evaluating the blended learning approach at Level 3 utilizing both e-learning and classroom learning. Blended learning incorporates delivery methodologies that respond to a variety of learning styles. Some learners need time to process information and

review content independently while others may prefer a real-time, interactive situation in which ideas and feedback can be exchanged face-to-face.

Another suggestion would be to launch the survey one month after completion of the training and then again after six months. The survey results after one month would most likely give better responses to questions such as *what specific suggestions do you have for improving this training*.

The researcher also recommends that the study could be taken a step further to conduct a Level 4 evaluation from six to twelve months post-training. Level 4 evaluations will report if there has been a return on investment (ROI). As with all research, the findings of this study should be utilized to solve problems for future research.

Summary

Due to recent advances in computer technologies, there has been an increase in e-learning methodologies for work-related training. Sloman (2002) indicates that while the practice of using computer and communication technologies for organization training has expanded rapidly, research examining the effectiveness of e-learning has lagged behind. In order to improve performance in the workplace, training must be transferred to the job. According to Broad (2005), transfer is the effective and continuing application by trainees of the knowledge and skills gained in training to the workplace. This study was conducted in response to the need for research in the effectiveness of e-learning and transfer of knowledge to the workplace.

When employers have invested in training and find that those employees have not applied the training back on the job, employers have lost time, money, and confidence in training as a viable business investment (Broad & Newstrom, 1992). In order to determine the effectiveness of e-learning, evaluation methods need to be engaged.

The Kirkpatrick model is often used for measuring the effectiveness of e-learning programs. This study concentrated on Level 3, which measures behavioral change on the job and includes specific application of the special knowledge or skills learned in the training. Level 3 typically includes self reporting from the learners and their supervisors and is measured after the training has been implemented in the work setting. Evaluation at this level may provide data that indicate the frequency and effectiveness of the on-the-job application and address why the application is or is not working as intended.

Although Level 3 evaluation is important in determining the application of the training, it still does not guarantee that there will be a positive impact on the organization. However, aligning the training with the strategic goals of an organization prior to the development of the Level 3 evaluation will result in the ability to measure performance improvement based on behavior change. Few studies have explored the link between training and corporate strategy.

This study focused specifically on e-learning for IT personnel of a utility company in Florida. Survey data were analyzed from the employees based on their experiences with a mandated online training course titled *Information Security Awareness Training*. There were 145 surveys completed and overall, the online training course feedback was very positive. Participants indicated that the training was relevant to their

jobs, felt that they were successful in understanding the objectives of the training course and gave candid responses to the open-ended questions.

More specifically, over 95% were successful in understanding company policies, the difference between strong and weak passwords and the dangers of computer viruses, worms and trojan horses. Social engineering was found to be the weakest area where 18% had limited to no success in understanding this objective.

In general, participants were clear before the training on the company policies such as installing unapproved software where 30% did not have the opportunity to apply the concept and 32% stated that there was no change in their level of improvement. A total of 79% had no opportunity to apply the policy of coordinating the installation of a DSL. It might be interesting to launch the survey after one year of training completion to determine if any of these objectives have been applied. There is a possibility that six months was not enough time for employees to actually apply all of the objectives that they learned in the training, although only 15% stated that they have not had enough time to apply the skills. This is even more reason to have ongoing reinforcement such as job aids, online peer discussions, etc. once the training has completed.

About 42% already understood that destruction of confidential records must be done with some form of disintegration such as shredding. A total of 22% made a significant change in that area, which can be viewed as a significant behavior change due to the training and consequently, should decrease the risk of identify fraud.

The free-form text responses provided a method to analyze changes that might be needed for the next iteration of the survey instrument. In addition, many of the participants indicated that this training was a beneficial reinforcement and refresher of

security practices. A total of 94% stated that the training was a good investment for the company.

The main purpose of the study was to produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies. In summary, the following measures have been recommended to achieve this goal. First, the online training should be aligned with organizational goals. Next step is to develop an overall strategic theme and break that down into relevant strategic sub-themes.

The balanced scorecard approach was introduced to affix accountability, track performance, and recognize achievement. The study reviewed the current IT department's BSC and determined that there is not a clear link to overall corporate strategy. A method to develop a measure such as strategy maps that depict overall organization strategic themes was recommended to improve the link between training and corporate strategy. By utilizing the BCS methodology, corporate strategies can be presented in a way that they can guide the content and skills acquisition of e-learning.

Finally, a survey instrument based on the objectives from the strategic sub-themes can be created. At first, the instrument may be a continual work-in-progress. If the survey instrument is broken down by strategic sub-themes it should become quite obvious if there were improvements as a result of the training. Analyzing the collected data may depict in certain areas that there was not as much of a performance gap as previously thought.

The results combined with the literature on the subject will be useful to training organizations within companies. The findings were used to develop guidelines to

produce a valid and reliable instrument to measure the alignment of IT e-learning with corporate and departmental strategies.

APPENDIX A
Sample Impact Questionnaire

Leadership Development Program Impact Questionnaire

Are you currently in a supervisory or management role/capacity? Yes No

1. Listed below are the objectives of the Leadership Program. After reflecting on the program, please indicate your degree of success in achieving these objectives. *Please check the appropriate response beside each item.*

Skill/Behavior	No Success	Very Little Success	Limited Success	Generally Successful	Completely Successful
A. Apply the 11-step goal-setting process	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B. Apply the 12 - step leadership planning process	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
C. Identify the 12 core competencies of outstanding leaders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
D. Identify 10 ways to create higher levels of employee loyalty and satisfaction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E. Apply the concept of Deferred Judgment in five scenarios	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
F. Apply the creative problem-solving process to an identified problem	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G. Identify the 7 best ways to build positive relationships	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
H. Given a work setting situation, apply the four-step approach to deal with errors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I. Practice 6 ways to improve					

communication effectiveness

2. Did you implement on-the-job action plans as part of the Leadership Program?
 Yes No

If yes, complete and return your Action Plans with this questionnaire. If not, please explain why you did not complete your Action Plans.

3. Please rate, on a scale of 1-5, the relevance of each of the program elements to your job, with (1) indicating no relevance, and (5) indicating very relevant.

	No Relevance	Some Relevance	Very Relevant		
Group (Class) Discussions	1	2	3	4	5
Small Team Discussions	1	2	3	4	5
Skill Exercises (scenarios, role plays, etc.)	1	2	3	4	5
Program Content	1	2	3	4	5
Coaching and critique)	1	2	3	4	5
Special Projects (leadership plan, job description, time log, money saving, etc.)	1	2	3	4	5

4. Have you used the written materials since you participated in the program?
 Yes No

Please explain.

5. In the following result areas, please indicate your level of improvement during the last few months as influenced by your participation in the Leadership Program.
Check the appropriate response beside each item.

Result Area	No Opportunity to Apply	No Change	Some Change	Moderate Change	Significant Change	Very Significant Change
A. ORGANIZING						
1) Prioritizing daily activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2) Applying creative techniques	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3) Organizing daily activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4) Raising level of performance						

6. List the three (3) behaviors or skills from the above list that you have used most frequently as a result of the program.

A) _____

B) _____

C) _____

7. What has changed about you or your work as a result of your participation in this program? (specific behavior change such as; increased delegation to employees, improved communication with employees, employee participation in decision making, improved problem solving, etc.) _____

8. How has your organization benefited from your participation in the program? Please identify specific business accomplishments or improvements that you believe are linked to participation in this program; (Think about how the improvements actually resulted in influencing business measures such as; increased revenue, increased overall shipments, improved customer satisfaction, improved employee satisfaction, decreased costs, saved time, etc.) _____

9. Reflect on your specific business accomplishments/improvements as stated above and think of specific ways that you can convert your accomplishments into a monetary value. Along with the monetary value, please indicate your basis for the calculations.

Estimated monetary amount \$ _____

Indicate if above amount is weekly, monthly, quarterly, or annually.

- Weekly Monthly Quarterly Annually

What is your basis for your estimates? (What influenced the benefits/savings and how did you arrive at the value above)?

10. What level of confidence do you place on the above estimations?

▶ _____ % Confidence (0% = No Confidence, and 100% = Certainty)

11. What percentage of the improvement above was actually influenced by the application of knowledge and skills from the *Leadership Program*?

▶ _____ % improvement (0% = None, and 100% = All)

12. Do you think this *Leadership Program* represented a good investment for your organization?

Yes No

Please explain. _____

13. Indicate the extent to which you think your application of knowledge, skills and behavior learned from the *Leadership Program* had a positive influence on the following business measures in your own work or your work unit. *Please check the appropriate response beside each measure.*

Business Measure	Not Applicable	Applies But No Influence	Some Influence	Moderate Influence	Significant Influence	Very Significant Influence
A. Work output	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B. Quality	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
C. Cost control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
D. Efficiency	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E. Response time to Customers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
F. Cycle time of products	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G. Sales	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
H. Employee turnover	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I. Employee absenteeism	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

(Continued) Applies Very

Business Measure	Not Applicable	But No Influence	Some Influence	Moderate Influence	Significant Influence	Significant Influence
J. Employee satisfaction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K. Employee complaints	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
L. Customer satisfaction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
M. Customer complaints	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
N. Other (please specify)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please cite specific examples or provide more details:

14. What additional benefits have been derived from this program?

15. What barriers, if any, have you encountered that have prevented you from using skills/behaviors gained in the Leadership Program? *Check all that apply.*

- I have had no opportunity to use the skills
- I have not had enough time to apply the skills
- My work environment does not support the use of these skills/behaviors
- My supervisor does not support this type of program
- This material does not apply to my job situation
- Other (please specify):

If any of the above checked, please explain if possible.

16. What enablers, if any, are present to help you use the skills or knowledge gained from this program? Please explain.

17. What additional support could be provided by management that would influence your ability to apply the skills and knowledge learned from the program?

18. What additional solutions do you recommend that would help to achieve the same business results that the *Leadership Program* has influenced?

19. Would you recommend the Leadership Program to others?
Yes No

Please explain. If no, why not? If yes, what groups/jobs and why? _____

20. What specific suggestions do you have for improving this program?

21. Other Comments: _____

From “*How to Measure Training Results*,” by J. J. Phillips and R. D. Stone, 2003, www.books.mcgraw-hill.com/training/download ; <http://books.mcgraw-hill.com/training/download/0071387927/> , p. 125.

APPENDIX B

Zoomerang Survey Instrument

Information Security Awareness Training Impact Questionnaire

1

Are you currently in a supervisory or management role/capacity?

YES NO

2

Listed below are the objectives of the Information Security Awareness Training. After reflecting on the program, please indicate your **degree of success** in achieving these objectives.

1	2	3	4	5
No Success	Very Little Success	Limited Success	Generally Successful	Completely Successful

Have an overall understanding of company policies and that inadvertent or accidental violation of security policy will result in penalties

1 2 3 4 5

Understand the difference between strong and weak passwords

1 2 3 4 5

Realize ways that Viruses, Worms, and Trojan Horses can get loaded onto your computer without your knowledge

1 2 3 4 5

Awareness of Adware, Spyware and Phishing and describe the dangers of each

1 2 3 4 5

Define and recognize instances of social engineering and outline how to respond if you are the victim of an attack

1 2 3 4 5

Describe Data Protection, identify customer and personal data, and summarize company data handling procedures

1 2 3 4 5

3

Did you implement on-the-job action plans as part of the Information Security Awareness Training?

YES NO

In the following result areas (#4 - #7), please indicate your level of improvement during the last few months as influenced by your participation in the Information Security Awareness Training.

4

Company Policies

1 No Opportunity to Apply 2 No Change 3 Some Change 4 Moderate Change 5 Significant Change

Installing unapproved software

1 2 3 4 5

Connecting to untrustworthy networks

1 2 3 4 5

Limiting personal use of company assets to appropriate use during approved times

1 2 3 4 5

Using email for sending or receiving junk mail

1 2 3 4 5

Coordinating the installation of DSL lines or wireless access points through computer support

1 2 3 4 5

5

Passwords and Social Engineering1
No Opportunity to
Apply2
No
Change3
Some
Change4
Moderate
Change5
Significant
Change

Not enabling any software application or web browser to "remember or save" your password

1

2

3

4

5

Not storing passwords in an obvious place such as posted on a monitor

1

2

3

4

5

Awareness of non-technical related issues such as impersonation of another employee

1

2

3

4

5

Awareness of the concept of shoulder surfing

1

2

3

4

5

6

Viruses, Worms, Adware and Spyware1
No Opportunity to
Apply2
No
Change3
Some
Change4
Moderate
Change5
Significant
Change

If the antivirus software icon has an error, call the help desk

1

2

3

4

5

Send hoax emails to the "Spam email" address and then delete it

1

2

3

4

5

Recognize Spyware such as pop-up ads

1

2

3

4

5

Recognize if a computer's performance is unexpectedly slow

1

2

3

4

5

Delete emails that have attachments that you did not request

1 2 3 4 5

Do not click on links embedded in emails

1 2 3 4 5

7

Data Protection

1 No Opportunity to Apply 2 No Change 3 Some Change 4 Moderate Change 5 Significant Change

Increased awareness that the company is an attractive target for identity theft fraudsters

1 2 3 4 5

Destruction of confidential records must be done with some form of disintegration such as shredding

1 2 3 4 5

Understand the company is responsible for protecting data such as social security numbers, bank information, date of birth and driver license information

1 2 3 4 5

8

List the three (3) behaviors or skills from the above list that you have been made most aware of as a result of the training.

Skill/Behavior 1

Skill/Behavior 2

Skill/Behavior 3

9

How has the company benefited from your participation in the training? Please identify specific business improvements that you believe are linked to participation in the training.

10

What has changed about you or your work as a result of your participation in the training?

11

Do you think this Information Security Awareness Training represented a good investment for the company?

12

What barriers, if any, have you encountered that have prevented you from using the skills/behaviors gained in the Information Security Awareness Training? Check all that apply.

- I have had no opportunity to use the skills
- I have not had enough time to apply the skills
- My work environment does not require me to use these skills/behaviors
- This material does not apply to my job situation
- Other, please specify

13

What additional support could be provided by management that would

influence your ability to apply the skills and knowledge learned from the training?

14

Did your supervisor discuss the training with you after you completed the program?

If "yes", please indicate one or two points that you recall from that discussion:

15

Was other support or encouragement received for applying the training?

16

What specific topics were **not** covered that you felt should be?

17

What specific suggestions do you have for improving this training?

18

Other Comments:



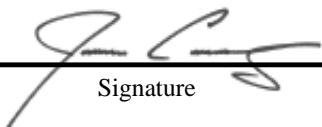
APPENDIX C
Institutional Review Board Approval

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board



MEMORANDUM

To: Heidi Kramer
From: James Cannady, Ph.D.
Institutional Review Board



Signature

Date: February 15, 2007

Re: *Measuring the Effect of E-Learning on Job Performance*

IRB Approval Number: cannady02150703

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

- 1) **CONSENT:** If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE REACTIONS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2085 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

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

Cc: Protocol File
Office of Grants and Contracts (if study is funded)

APPENDIX D

Survey Consent Letter

Dear Colleague,

I am soliciting your participation in my doctoral research at Nova Southeastern University. I am conducting a research survey that will seek to gain knowledge about the alignment of IT e-learning with corporate and departmental strategies. You have been selected to partake in this survey because of your participation in the Information Security Awareness Online Training course. Please take a few moments to complete this survey. Your participation in this survey is both optional and anonymous.

In addition to the doctoral research, Information Security management will also be reviewing the results of the study. If you have any questions or are interested in the results of this study, please contact me at heidi_kramer@xxx.com.

I appreciate your willingness to assist me in this effort.

Sincerely,
Heidi Kramer

APPENDIX E

Results and Responses from Question #8

Question 8: Skill/Behavior 1	Question 8: Skill/Behavior 2	Question 8: Skill/Behavior 3
Ad-ware, Spy-ware	Send spam emails to spam address	more in tune with password policys
aware of all of them before any training		
Better communication re: security	More scrutiny of external e-mails and web-sites	
Better passwords	Antivirus software	Concept of shoulder surfing
Carefully disposing of sensitive data	Phishing scams	Spyware programs
company is a target for identity theft	difference between worms, viruses and trojan horse	understanding social engineering
COMPANY POLICIES	DATA PROTECTION	PASSWORDS
Company Policies	Passwords and Social engineering	Data Protection
Company Policies	Data Protection	Viruses, worms, etc.
Company sensitive data	Delete unsolicited emails	Recognize popup ads as possible spyware
complex password	social engr	data protection
creating strong passwords	better awareness of emails from unknown authors	making sure to lock ws when walking away from desk
Data Protection		
DATA PROTECTION	VIRUSES WORMS	PASSWORDS
DATA PROTECTION	PASSWORD AND SOCIAL ENGINEERING	COMPANY POLICY
Data Protection	Shoulder surfing	Not storing passwords in obvious places
Data Protection	Company Policy	Password and Social Engineering
Data Protection for cust and company records	Aware of Social Engineering	Strong passwords
Delete emails that have attachments that you did n	Not enabling any software application or web brows	Connecting to untrustworthy networks
Delete emails that have attachments that you did n	Connecting to untrustworthy networks	Installing unapproved software
Destruction of confidential records	Protection of data such as social security numbers	Send hoax emails to the "Spam email" address

Destruction of confidential records (shredding)	Deleting email w/ attachments that are not recogni	
Destruction of confidential records must be done	Delete emails that have attachments that you did n	Understand the company is repsonible for protect
detection	solution	implementation
Do not click on embedded links in emails	Do not allow the system to "save" my password	
do not open email from unknown source		
DO NOT OPEN THE ATTACHEMENT FROM UNKNOW EMAIL	PASSWORD MUST COMBINE OF NUMBER AND CHAR	
email attachments	passwords	security measures
Establishing a Strong Password	Awareness of Shoulder Surfing	Awareness of Phishing
Handling of unsolicited emails	The whole idea of social engineering	good vs not-so-good passwords
I already knew about everything covered.		
I put no change because I behave accordingly		
Identity theft	Data protection	Social Engineering
Implemented shredding of documents as needed	More aware of spyware & pop-up issues	More aware of importance of protecting cust info
Increased awareness		
Increased awareness that FPL can be a target	The concept of shoulder surfing	General reinforcement of good Info Sec practices.
Increased awareness that the company is an attract	Delete emails that have attachments that you did n	Using email for sending or receiving junk mail
Installation of unapproved software	Connecting to an untrusted network	Limited personal us of company assets
Junk emails	storing passwords	personal data protection
Limiting personal use of company assets to appropri	Awareness of the concept of shoulder surfing	Do not click on links embedded in emails
Making Passwords harder	Understanding Viruses better	Smarter use of company assets
Need for proper passwords		
No saving passwords in applications.	Don't download unauthorized software.	Make passwords more difficult.
none	none	none
None, I was already aware of them		

Not allowing application to remember password	strong/weak passwords	social engineering/impersonation
Not enabling any software application or web brows	Send hoax emails to the "Spam email" address and t	Delete emails that have attachments that you did n
overall understanding of company policies		
password	when leaving my workstation press lock desktop	do not access internet from work
password changes	password complexity	downloading software
password protection	delete unknown email with attachments	protecting company data
Password recall		
password security	fraud emails	unexpected attachments
password selection	virus protection	corp policies
password social engineering	data protection	virus worms adware
Password Strength	Virus and worm section	Social engineering
passwords and social engineering		
passwords and social engineering	data protection	virus and spyware
Phishing		
Phishing	adware/spyware	Data protection
phishing	securing comopany data	destruction of hard drives on outdated equipment
Protect all employee data	Do not visit untrustworthy websites	desctructing confidential records
Protecting Social Security numbers	Do not click on embedded emails	Do not open emails not recognized w/attachment
Protection of private information	Social Engineering	Virus types
Recognize junk email pop ups	do not click on any unknown links	avoid any shoulder surfing
Recognize spyware	Using strong passwords	Send hoax e-mails to spam e-mails
Restricting application access to sensitive info	Shred documents with sensitive info	Delete e-mails from unknown sources
Send all unknown e-mail to Spam	Aware if company is a target for identity theft	Recognize computers performance is slow
send hoax email to "spam email"	antivirus icon notify help desk	awareness of shoulder surfing
Send hoax emails to the "Spam email" address and t	Understand the company is repsonsible for protecti	
send spam to SPAM email	shoulder surfing	storing passwords securely

shoulder surfing		
Shoulder Surfing	Company Policies	E-mail for sending/receiving junk mail
Shoulder surfing		
shoulder surfing	social engineering	
slow computer operation	shred documents	send spam to spam file
smart passwords		
social engineering	data encryption	shredding confidential data
Social engineering	Difference between strong and weak passwords	Shoulder surfing
Social Engineering		
Social Engineering	Installing Unapproved Software	Difference Between Strong and Weak Passwords
social engineering	phishing	installation of dsl lines
social engineering	shoulder surfing	
social engineering	adware/spyware	viruses
Social Engineering		
SPAM EMAIL	COMPUTER PERFORMANCE	ATTACHMENTS
Spam email	Strong Passwords	Viruses
Spyware	Passwords	Impersonation
storage of password	delete unrequested emails with attachments	protecting confidential information
Strong passwords	Social Engineering	Viruses and trojans
Treatment of sensitive data	Action taken regarding SPAM emails	Awareness of shoulder surfing
Understand the difference b/w good/bad passwords.	Delete emails that have attachments not requested.	Connecting to untrustworthy networks.
Undestand data protection	Destruction of confidential records	
Verify who people are		
Virus protection for users	Destruction of Confidential Materials	Awareness of Theft Fraud
Viruses, Worms, Adware and Spyware	Awareness of non-technical related issues such as	
Viruses, Worms, Adware and Spyware	Data Protection	Passwords and Social Engineering
Viruses,Worms,Adware,and Spyware	Company Policies	Data Protection
Weak & Strong Passwords	Using e-mail for sending or receiving junk mail	Define & recognize instances of social engineering

what list?		
------------	--	--

Tallied responses from Question #8

All responses from Question # 8 that stated to list 3 behaviors or skills from the above list that you have been made most aware of as a result of the training		
aware of all of them before any training	4	Aware
don't access internet from work	1	Company Policies
lock desktop	2	Company Policies
limiting person use of company assets to appropriate	3	Company Policies
connect to untrustworthy networks	5	Company Policies
company policies	9	Company Policies
don't open email from unknown source	10	Company Policies
identity theft	2	Data Protection
company sensitive data	5	Data Protection
company target for identity theft	5	Data Protection
disposing of sensitive data	11	Data Protection
data protection	28	Data Protection
storing passwords	1	Passwords & SE
impersonation	1	Passwords & SE
save password	3	Passwords & SE
shoulder surfing	15	Passwords & SE
social engineering	23	Passwords & SE
complex password	37	Passwords & SE
better communication	1	unknown
destruction of hard drives on outdated equipment	1	unknown
spam to spam address	2	Viruses
unknown links	2	Viruses
slow computer operation	3	Viruses
phishing	5	Viruses
worms, virus & trojan	6	Viruses
antivirus software	7	Viruses
enabling software application or web browser	8	Viruses
send spam emails	13	Viruses
Adware, spyware	14	Viruses
delete emails with attachments'	15	Viruses
TOTAL	242	
Passwords	80	33%
Unknown	2	1%
Viruses	75	31%
Already aware	4	2%
Company Policies	30	12%
Data Protection	51	21%
Total	242	100%

APPENDIX F

Responses from Question #9

Question 9: How has the company benefited from your participation in the training? Please identify specific business improvements that you believe are linked to participation in the training.
1. Employee awareness has increased; however, it may be good to have a refresher in the future as we tend to forget the material after time has passed.
a general awareness of security as it pertains to computer processing
All passwords now pass the company requirements for secure passwords
Avoids hackers from obtaining access to our environment.
Aware now of all dangers outside sources use to try to access confidential material.
Awareness of issues important to the company from a security standpoint.
Awareness.
be more aware of what security means, password, data security, etc...
Being in a support role, I know now what to look for when I receive certain tickets indicating slow performance.
better business relationships, better secured environments, easily locate and regulate the spammed and junk emails
Better safe keeping practices
better security of network
better understanding, prepared for questions, security, password issues.
Bringing awareness is important. If employees are not educated on how there actions can affect the corporation, they won't know to change their actions.
Broader awareness of the issues & impacts.
Communicated to my employees and this will reduce the desktop support tickets.
Desktop is better protected from corruption as well as users.
Destruction of confidential records must Making sure that confidential records are shredded.
did not
Email system is available 100% of the time
ensured all employees had similiar understanding
Even with good habits, reinforce the need to be vigilant and thinking about risks
General Awareness of tactics used by criminals to attain confidential information
General awareness of total security

Generally speaking was fully aware of all relevant issues. Awareness training reinforced policies already in place and few changes were required. Reminders of potential pitfalls and possible issues was useful but not new knowledge.

We did implement a shredding policy to insure that documents containing sensitive company or customer info no longer needed were destroyed rather than thrown out intact.

greater awareness

Greater awareness of security related issues

heightened awareness

Heightened awareness of threats to the company.

Higher level of awareness that company data is actively being sought by folks that want to exploit that knowledge.

I am a smarter internet user

I am sure that I have been following these suggestions on my own for many years prior to this class

I feel I have always been very savvy at security awareness... this is why I responded; "some change". However, I feel the training is a great refresher and if anything to increase awareness, we can never be too careful!

I follow the employee guideline which describe many of the Info Security awareness.

I have always followed the appropriate policy even before these were published.

I like to think that I already engaged in secure practices, particularly in terms of using strong passwords and securing my assets.

I no longer allows the system to save my passwords.

I think for the non technical audience, this was a good training.

I was aware of most of practices used to steal personal information, but the course did refresh my memory.

I was aware of most of these things prior to the training

I was previously aware of all these items and already very cautious of them so no real change was needed, however I am a minority the general end user is not aware. Business improvement comes from awareness of the general public. Especially, regarding spam and downloads.

I was security aware before training, it is business as usual

I'm more security conscious.

improved security

Increased awareness of Sensitive information.

Information refresher.

It reminded me of many factors I already knew, and enlightened me on some techniques I was not familiar with.

It's good to keep these issue in the spotlight

Just increased awareness...I've always been aware and done the things necessary.

Make me aware of personal and company sensitive information.
More aware of potential risks to company assets.
More aware of social engineering, difference between strong and weak passwords
More aware of the company's exposure to risk involved with virus and the necessary precautions required to help prevent them.
MORE AWARENESS ABOUT SECURITY IN GENERAL
More awareness of security threats. It was also a good review and reinforcement.
More careful about when I use the internet and for what reasons.
MORE KEENLY AWARE OF ITEMS LISTED IN SKILL/BEHAVIOR 1-3
More security-aware.
my computer is virus free and has not infected teh network
My spam management is better now
n/a
NA
na
None
None. Already adhering to company policies and procedures.
Not much as I was aware of these items before the training and was taking the proper precautions
not sure. a lot of these things are common sense. i guess it's a standard awareness for everyone.
Overall increase in awareness and action/reaction to possible breaches of security.
Personaly no improvement as I was already aware, but I think some people will benefit
Raised the awareness level for security and improved the alertness for malicious or suspicious e-mails.
Raised the level of existing awareness.
Reduced risk of security issues
Reinforced the security concepts I already practice. Reviewed the areas covered by the security policy.
Removed or reduced the amount of suspect software from customer devices.
SAFEGUARD CUSTOMER'S CONFIDENTIALITY
Securing Company infurstracter.
See below
talked to others about the training..
The company should continue this education outside of IM for the less savvy users.
The more people are aware of the policies the safer our vacation will be.
This training reinforces standard protocols
Trainging customers, about virus, that I am in contact with
Unknown
use internet less for frivolous searching and use it more strictly for business research

Using better passwords
Using strong passwords.
We all have the responsibility of helping to protect the business
Will limit internet use
yes
Yes
Yes, although most of this is common-sense, it helps to reinforce.
yes, i am part of the data encryption project and training has re-emphasized the risks that need to be mitigated.
yes, the company network is now safe.
Yes, there is now available document destruction service for important files

Appendix G

Responses from Question #10

Question 10: What has changed about you or your work as a result of your participation in the training?
a higher degree of awarness
a better awareness of securing my surroundings.
Am more careful in my internet usage
Awareness
awareness
Awareness of the sensitivity of data we deal with.
become more cautious with use of internet
Being part of the IMSC having the tools to secure our work place.
Better awareness of spam emails
Better safe keeping pratices as they pretain to securing information
Both my job and education are related to security issues. I was already familiar with most of the training outlined in the course and the different methods for compromising computer resources. But it was a good opportunity to refresh the concepts
creating passwords, protecting my desktop when leaving, to going to the internet if not work related.
GET AWARENESS OVVERALL.
greater awareness
greater awareness
I already practice good security.
I always lock my keyboard when I leave my desk.
I am even more aware than in the past of security issues.
I am mindful of the damages that viruses, etc can cause and cost the company.
I am more aware of emails I open and sites I visit.
I am more cautious
I am more cautious about who I talk with over the phone. I am more careful of company documents.
I am more coutious and aware of what I am doing. I don't take anything for granted.
I am sure that I have been folloing these suggestions on my own for many years prior to this class
I check web site in more details to ensure they are not phishing sites
I contribute to making FPL's network secure and virus-free
I don't send junk emails
I lock my workstation more frequently
I no longer allows the system to save my passwords. I used to do this to make it easier for me.
i no longer open emails from senders that i do not recognize. i also try to notify info sec of any suspicious emails.

I think I had a high pre-existing awareness of the Security issues covered by the course. Therefore, whereas I think the course is worthwhile, I did not benefit significantly.
I very rarely used the Internet before the training, now I never use it.
I was already aware and adhering to most of the information provided in the training; therefore, most answers might indicate no change or no opportunity to apply
Increase awareness to different risks
Increased awareness
Increased awareness of Sensitive information.
increased awareness!
Increased shredding of documents with company or customer information
It has ensured that i should always be aware of these security challenges
It was a good overview for employees
I've been aware of many, if not all, of the security awareness..
Less personal email
Limiting personal use of company assets to appropriate use during approved times
More acutely aware of what might infect my company machine and the network
MORE ALERT ABOUT PROTECTING MY OWN DATA
More aware of potential threats, methods of attack
More aware of secure protection of customer and my own information
More aware on company policies and how they are applied
More aware.
More awareness
More care taken in email management of junk mail, spam, etc.
more carefull to use safe sites
More Cautions connecting to unknown networks. Still could give more indepth guidelines regarding this. Since when traveling for business every hotel, conference center and airport has wifi now. We need to know if it's ever ok to connect.
More cautious about how I use comapny assets.
More cautious about password protection.
More cautious about possible hazards.
More cautious about sensitive information.
More cognizant of safe guarding electronic information,
More conscious about locking terminal when leaving my desk.
More in tune with what would be sensitive data if it went out of FPL
More knowledgable and more aware.
More security awareness than before.
More vigilant and communicate to customers importance of strong passwords.
More vigilant of how viruses could be spread i.e be careful when handling unknown e-mails.

More wary about sharing data about customer information.
My workstation is protected all the time.
Never break security policies.
No change.
no changes, but re-enforced need for safeguards in place
No changes.
None,
Not much change due to prior awareness and action.
Not much, I feel that I was already practicing secure habits.
not much, I knew most if not all of it from before. Again, I think this was more beneficial for non IT audience than the IT population, but it was informative non the less.
Not much.
Not using thumb drives for file backups and data sharing.
Nothing
nothing
nothing
Nothing
Nothing has changed
Nothing really, just more enlightened.
Nothing, I was always aware of these issues.
password selection and knowing how viruses are spread.
Pay closer attention to e-mails and use shredder for sensitive data.
poor attitude
Prompted discussions with my employees about Security issues that they were not aware of.
Purposely look away when customer's are entering their passwords.
Reduce the number of tier 2 support tickets to fix or repair laptops and workstations.
reinforced topics that I deal with day to day
run ad-aware & spybot more often
safe usage of information due to protection from spamming, viruses etc.
security awareness
Somewhat
Taking less risk with external sites/e-mails
Using more spyware
Using stronger passwords
very little. But I feel that I was already educated.
Very little. In Ques 4-7 above, there was little change since I employed most or all of the suggestions before the training. The training served to enforce pre-existing habits.
watching my shoulders
We treat emails from outside sources with more suspicion

When I receive phone calls from unidentified callers that are requesting another employee # or extension, I make sure that I do not provide the caller with any information.

Work habits have not changed - I was already aware of security concerns at FPL

WORKSTATION IS NO LONGER LEFT ACTIVE WHEN NOT AT MY DESK EVEN IF FOR A MINUTE.

APPENDIX H

Responses to Survey Question #12

Question 12: Other, please specify
Already very security-minded prior to training
ease for shredding of sensitive documents
Good practices are not embedded into our culture
Had prior knowledge
hard to remember multiple 'smart' passwords
Helps with CU service
I already apply the applicable skills daily
I already did these things
I already use some of the skills/behaviors
I am able or required to apply all techniques.
I am sure that I have been following these suggestions
I have applied where applicable
I have not had an opportunity to use all the skills
I haven't encountered any barriers.
I observe these measures on a daily basis
I've always been tuned to these issues.
Lack of processes to overcome needs of job
More difficulty in rolling out new It's and ws's
My job requested Information Security Awareness
N/A
n/a
N/A
n/a
No Barriers
No barriers
no barriers
No barriers
no barriers
No Barriers
no barriers encountered
No barriers. Fortunately, not experienced issue.
No single sign-on,
none
None
none

None
None
none
none
none
none
none
none
none
None encountered
none of the above
None.
Not applicable - no barriers encountered.
Our SPAM filter could use more improvement...
remembering hundreds of passwords is difficult
This information was already being applied.
Too difficult to remember strong passwords
too many people have admin rights
was aware of these issues already

APPENDIX I

Responses to Survey Question #13

Question 13: What additional support could be provided by management that would influence your ability to apply the skills and knowledge learned from the training?
ALLOCATED TRAINING TIME FOR EACH EMPLOYEE WHENEVER THE CO INTRODUCE NEW SECURITY TRAINIGN MATERIAL.
Better SPAM filter control...
cannot think of anything
Communicate to all business units.
DON'T KNOW
dont threaten employees for accidently violating security policy resulting in penalties.
enforce them.
Follow-up training or discussion.
For whatever access is restricted, there's needs to be a way to execute valid business delivery
High level review in staff meeting. Periodically bringing up key points of the training.
I am already utilizing the skills gained.
I am sure that I have been folloing these suggestions on my own for many years prior to this class
Identify and inform IMSC immediately with any type of security breaches from internet (if any), caused during the work so that IMSC takes care of preventing them from further causing damage to company's assets.
if while 'cleaning-up' users pc i was allowed to delete non approved software and a letter was sent by im security as a follow-up
Implemt Single Signon, too many systems too many password
Keep current on latest Virus/spyware software.
Keep up the awareness, just like anything else this is one more issue that will fade unless kept current.
management get more involved
Maybe some sort of initial info sec class when employees are first hired, especially when they get promoted to higher positions that gives them more access and responsibility
method of keeping track of hundreds of passwords for multiple systems
More reinforcement of the informatio in the training.
More training
More training, tips and tricks
N/A
n/a

n/a
N/A
n/a
N/A
n/a
n/a
na
na
No ideas at the moment
none
none
none
none
None
none
None
none
none
None
none
none
None
None I'm aware of
none. was self explanatory
Not Applicable
O do not foresee any additional support helping, because I do not really have time to experience all security issues.
Offer more training to new hires on basic computer usage and explain the policies to them fully. Not just an on-line course to be taken.
Provide live examples of what has happened in real world situation , like what happened with a credit agency when they gave the info for 1/2 million customers out by an error,and that real people had to undergo so much for no mistake of theirs.
Refresher every 1 or 2 year will be helpful.
Reminders about the dangers of emails and other data sources from outside the company
Reminders.
Request customer's take the test (refresher) each year.
Require refresher training on yearly basis for all employees.
Short, brief reminde. SHort is the key phrase. The initila training was way to long.
Since more and more employees are using remote access with their personnel machines, IM may want to provide a more enhanced version of Norton for home use

Some occasional reinforcement via e-mail, INFPL, or something similar

They could have a follow up mtg and discuss the terms learned again and provide examples on how to use them.
--

unknown

We are aware of sensitive data and management has taken actions to improve the security of that data.

APPENDIX J

Responses to Question #14

<p>Question 14: If "yes", please indicate one or two points that you recall from that discussion:</p>
<p>1. Safeguarding of customer information</p>
<p>2. Limiting personal use of company assests.</p>
<p>Be sure to keep all NPI data secure.</p>
<p>Do not open attachments from emails you do not know.</p>
<p>company Policies</p>
<p>Company Policy</p>
<p>data security , password settings</p>
<p>discussed in a staff meeting as a group</p>
<p>Don't request user passwords from customers.</p>
<p>Financial data must be guarded and protected at all times.</p>
<p>Identifying and informing the Supervisor with any type of security breach if come across during the work;</p>
<p>Data and Password protection ;</p>
<p>Do not surf to sites that cause Adware/Spyware to penetrate into the system etc.</p>
<p>If we encountered any of the examples.</p>
<p>Internet use should be for company business</p>
<p>just reiterated the importance of passwords and communicating to customers.</p>
<p>Lockdown of SSN information in applications, Shred sensitive reports, etc.</p>
<p>not necessary</p>
<p>Payt attention to it and support it in my organization</p>
<p>perform audit of supported applications for compliance</p>
<p>Reminders to be aware of specific external tactics employed by those seeking to invade the company's networks and information stores.</p>
<p>Strong Passwords, Spam email</p>
<p>To become familiar with the policies and procedures.</p>

Virus and Spyware installation for CU with LT problems
We covered all points in a staff meeting.
We had a presentation prior to the training covering attack types, social engineering, and private information protection needs.

APPENDIX K

Responses to Question #16

Question 16: What specific topics were not covered that you felt should be?
Best practices for personal data file protection
Don't know.
Don't recall anything.
employee recourse
how to better use internet options for security purposes
HOW TO PREVENT SPAM EMAIL.
I believe they were covered
Identity theft repair.
Is there a reference (hardcopy)booklet...? I completed the training a few months ago and do not recall every thing that was covered.
n/a
n/a
n/a
N/A
n/a
N/A
N/A
n/a
na
NA
na
No ideas at the moment
none
None
none
None
None
none
None
none
None
None
none
none
none

none
None I'm aware of
None.
pen files...
procedures for getting outside vendors network access while at FPL.
Security around Blackberry.
Setting up firewalls for home computers.
unknown
Use of "thumb" drives - I don't remember that being covered
Use of external memory media from home for working at work and home.
Yes, use of other media such as CD and DVD should be included in the list of media that must be DESTROYED. Also the disposal of cell phones/blackberries was not covered, there is a lot of information stored on these devices.

APPENDIX L

Responses to Question #17

Question 17: What specific suggestions do you have for improving this training?
A bit more information on how to protect your personal home computer.
dont threaten employees
Frequency, friendly reminders...
how to better use internet options for security purposes
I would suggest repeating the training every 6 months since the information is hard to remember if not reminded on a consistent basis.
include in the survey the possibility that the student knew the items in the training before he/she took your class....for example one of the butons should read "have been using this proceedure prior to this training" instead of assuming everyone that takes this training was totally oblivious to security as it relates to our network...
include non-fpl employees in taking this training class
Included more real live cases of companies being affected by not using these tools effectively.
Issue reminders, especially to our business personnel outside of IM
Maybe making it either more in depth for the IT group, or just giving it out to the rest of the company, but in any case, I am sure some of our co-workers in IT benefited form it if they were not aware of some of the things.
More realistic discussions of real world security breaches.
n/a
n/a
n/a
N/A
N/A
n/a
na
Needs to be more oncese
No ideas at the moment
None
None
none
None
NONE
none
None
none

None
None
none
none
None
None
none
none
None
None
none
none it was good
None, was very adequate
Nothing really. It is a good orientation for new employees to DP. However, after 38 years in DP it's hard to not understand these concepts...the review was useful.
require annually
See # 16.
The training was good and covered all the major points. A refresher course should be made available.
Training was fine.
unknown

APPENDIX M

Responses to Question #18

Question 18: Other Comments:
* I'm not sure I even remember taking this course. But I believe it was something that we may have taken several months ago (?)
* It always find it discouraging to see that we're taught something like "Do not click on links embedded in emails
", but then our own company does this regularly without any additional information. For example, every time we get a mass mailing, the email comes from someone we don't know, and in the body of the email, all it says is "Click here for more information." and then shows a Lotus Notes document link. How do I know that this is not spam? What identifies this mass mailing as something from the company instead of the outside? You don't know until *after* you click the link.
dont threaten employees
Facilities management should consider the people who come in to clean especailly behind locked doors. To me this is a concern with laptop theft and papers on desktop.
Great Training
I feel it is good over all for the company but working with the web daily exposes me to the situations.
In 4-7, there's no good answer if you already applying secure processes - "No opportunity to apply" is different than something like "Already employing concepts"
Levels of improvement do not really include a selection for negative behaviors that you did not previously do (and would not do in the future). Example: Installing unapproved software. I do not install and would not install unapproved software. What is the answer I should select? 1????
Management views these measures as "guidelines" instead of company policies and procedures and decides to pick and choose which ones should be followed.
Most of the anserts that I respoded no change were do to the fact that those processes were already in place, or I was aware of them.
n/a
n/a
N/A
None
None
NONE
none
none

None
none
None
none
None.
none.
Poor responses for survey questions (4-7). Responses to questions are very confusing and didn't make sense to me.
For example...#5
Question... Not storing passwords in an obvious place such as posted on a monitor.
My thought... I never posted passwords in an obvious place... nor would I.
If I select...
1. No Opportunity to Apply - I guess I don't use passwords?
2. No Change - I'm guessing this is the answer I should select.
3. Some Change - I post them on rare occasion?
4. Moderate Change - I post them only on occasion?
5. Significant Change - I only post them if I rarely use them?
Survey cannot be done in 5 minutes so please don't say 5 minutes, 10-15 is realistic.
The survey should have been sent out sooner because I remember taking the class but don't remember all of the details that well.
The training was good and applies to computing habits at work and at home. Working for IM, I already was aware of most of the information covered. This means my habits did not change much as a result of the training, but the refresher is good. Would be good to have updates for employees as the threat environment changes.
this survey was a bit confusing; the 1 - 5 numbers were difficult to interpret with regards to the behavior
totally one sided survey answers should

Reference List

- Adkins, S. (2003). ROI from workflow-based e-learning. *Learning Circuits*, Retrieved May 15, 2006, from www.learningcircuits.org/2003/oct2003/adkins.htm
- Allen, M. (2003). The lessons of e-learning. *Optimize (Issue 22)*, Retrieved, September 25, 2006, from <http://www.optimize.com/article/showArticle.jhtml;jsessionid=OIFD4C4ID505WQSNLPSKHSCJUNN2JVN?printableArticle=true&articleId=17701029&queryText=>
- American Society for Training and Development (2006). *Annual report of the industry*. Alexandria, VA.
- American Society for Training and Development (2003). *Annual report of the industry*. Alexandria, VA.
- Bahlis, J. (2006). Maximize training impact by aligning learning with business goals. *Presented at the Society for Applied Learning Technology (SALT) 2006 New Learning Technology Conference*, Retrieved July 19, 2007, from www.bnhexpertsoft.com/english/resources/whitepaper.htm
- Bassi, L., Ludwig, J., McMurrer, D. P. & Van Buren, M. (2000). Profiting from learning: do firms' investments in education and training pay off? *ASTD Research White Paper*, Retrieved March 4, 2006, from <http://www.astd.org/NR/rdonlyres/06811CDD-3143-4BD3-A76E-C0CEFF03040F/0/PFLWhitePaper.pdf>
- Beamish, N., Armistead, C., Watkinson, M., & Armfield, G. (2002). The deployment of e-learning in UK/European corporate organization. *European Business Journal*, 14(3), 105-115.
- Beasley, M., Chen, A., Nunez, K. & Wright, L. (2006). Working hand in hand: balanced scorecards and enterprise risk management. *Strategic Finance*, March(2006), 49-56.
- Bergman, P. & Jacobson, H. (2000). Yes, you can measure the business of results of training. *Training*, 13(13), 1-6.
- Bersin, J. (2002). Measure the metrics: how to link e-learning to business strategy. *LTi Magazine*, Retrieved May 15, 2006, from www.ltimagazine.com/ltimagazine/content/printcontentpopup.jsp?id=21256
- Brinkerhoff, R. O. (2002). Using evaluation to build organizational performance and learning capability: a strategy and a method. *Performance Improvement*, 41(6), 6-10.

- Brinkerhoff, R. O. (2005). The success case method: a strategic evaluation approach to increasing the value and effect of training. *Advances in Developing Human Resources*, 7(1), 86-101.
- Broad, M. L. (2005). *Beyond Transfer of Training*. San Francisco: Pfeiffer.
- Broad, M. L. & Newstrom, J. W. (1992). *Transfer of Training: Action-packed Strategies to Ensure High Payoff From Training Investments*. Reading, MA: Perseus Books.
- Brown, R. M. & Eggers, J. T. (2005). Management development for impact. *Corrections Today*, 67(7), 100-103.
- Burnett, K. & Subramaniam, M. (2004). Defining the information technology workforce from the educational perspectives: a pilot study. *Proceedings of the Special Interest Group Information Technology Education (SIGITE '04)*, ACM Press: New York, NY, pp. 202-205.
- Cegielski, C. G., Reithel, B. J. & Rebman, C. M. (2005). Emerging information technologies: developing a timely IT strategy. *Communications of the ACM*, 48(8), 113-117.
- Chevalier, R. (2004). Evaluation: the link between learning and performance. *Performance Improvement*, 43(4), 40-45.
- Cohen, S. L. & Backer, N. K. (1999). Making and mining intellectual capital: method or madness? *Training & Development*, 53(9), 46-47.
- Coverstone, P. D. (2003). IT training assessment and evaluation: a case study. *Proceedings of the 4th Conference on Information Technology Curriculum (CITC4'03)*, ACM Press: New York, NY, pp. 206-213.
- Creswell, J. W. (2005). *Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research* (2nd ed.). Upper Saddle River, NJ: Pearson / Merrill Prentice Hall.
- Cross, J. (2001). A fresh look at ROI – training return-on-investment meets the information age. *Learning Circuits*, Retrieved May 1, 2006, from www.learningcircuits.org/2001/jan2001/cross.html
- Cross, J. (2004). OpEd: ROI vs. Metrics. *Learning Circuits*, Retrieved September 26, 2006, from www.learningcircuits.org/2004/apr2004.cross.htm
- Dabbagh, N. & Bannan-Ritland, B. (2005). *Online Learning: Concepts, Strategies and Application*. NJ: Pearson Education, Inc.

- Dagada, R. & Jakovljevic, M. (2004). 'Where have all the trainers gone?' E-learning strategies and tools in the corporate training environment. *Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT '04)*, ACM Press: New York, NY, 194-203.
- Data privacy. (2007, June 11). In *Wikipedia, The Free Encyclopedia*. Retrieved 19:45, June 23, 2007, from http://en.wikipedia.org/w/index.php?title=Data_privacy&oldid=137456149
- Devaraj, S. & Babu, R. (2004). How to measure the relationship between training and job performance. *Communications of the ACM*, 47(5), 63-103.
- Denning, P. J. & Dunham, R. (2001). The cord of the third-wave professional. The IT profession is the first profession in the third wave of civilization. *Communications of the ACM*, 44(11), 21-25.
- Downey, J. (2005). A framework to elicit the skills needed for software development. *ACM Computer Personnel Research Conference (SIGMIS-CPR '05)*, ACM Press: New York, NY, 122-127.
- Egan, D., Hessian, D., Taylor, C. & Zenger, J. (2003). Suppliers: it's time to push e-learning and e-learning ROI up to the CEO level as a business investment versus a cost center. *T&D*, 57(1), 62-64.
- Eid, T. (2006, June 23). Findings: IT investments are aligning with business needs. *Gartner Research, ID Number: G00141364*, Retrieved August 1, 2006, from http://www.gartner.com/DisplayDocument?ref=g_search&id=493376&subref=simplesearch
- Feldman, S. & Bahr, M. (2004). A report of the task force on workforce development. *The Albert Shanker Institute and The New Economy Information Service*, Retrieved January 12, 2006, from <http://www.newecon.org/TFReport4-20-04.pdf>
- Fjermestad, J. & Saitta, J. A. (2005). A strategic management framework for IT outsourcing: a review of the literature and development of a success factors model. *Journal of Information Technology Case and Application Research*, 7(3), 62-60.
- Filho, W. A., Latham, L. & Lundy, J. (2006, February 22). E-learning key issues, 2006. *Gartner Research, ID Number: G00137917*, Retrieved, August 1, 2006, from http://www.gartner.com/DisplayDocument?ref=g_search&id=489459&subref=simplesearch

- Filho, W. A. (2005, December 8). Use e-learning to improve your business. *Gartner Research*, ID Number: G00136627, Retrieved, August 1, 2006, from http://www.gartner.com/DisplayDocument?ref=g_search&id=487155&subref=simplesearch
- Ford, D. J. (2004). Evaluating performance improvement. *Performance Improvement*, 43(1), 36-41.
- Fowler, F. J. (2002). *Survey Research Methods* (3rd ed.). Thousand Oaks, CA: Sage Publications.
- Gable, R. K., & Wolf, M. B. (1993). *Instrument Development in the Affective Domain: Measuring Attitudes and Values in Corporate and School Settings* (2nd ed.). Norwell, MA: Kluwer Academic.
- Gale, S. F. (2002, August). Measuring the ROI of e-learning. *Workforce*, 81(8), 74-76.
- Gay, L. R. & Airasian, P. (2003). *Educational Research: Competencies for Analysis and Applications*. New Jersey: Merrill Prentice Hall.
- Galloway, D. L. (2005). Evaluating distance delivery and e-learning: Is Kirkpatrick's model relevant? *Performance Improvement*, 44(4), 21-27.
- Goldwasser, D. (2001). Beyond ROI. *Training*, 38(1), 82-86.
- Goodridge, E. & Swanson, S. (2001). ROI boosts e-learning – online-training sales rise, even as it budgets are tightened. *Information Week*, (May 7, 2001), 135-136.
- Green, D. T. (2004). Corporate training programs: a study of the Kirkpatrick-Phillips model at Electronic Data Systems (Doctoral dissertation, Capella University, 2004). *Proquest Information and Learning*, UMI number: 3138944.
- Hall, B. & LeCavalier, J. (2000). The case for level 3. *Learning Circuits*, Retrieved May 1, 2006, from www.learningcircuits.org/2000/nov2000/hall.htm
- Harris, P. (2003). ROI of e-learning. *T&D*, 57(2), 30-37.
- Henneman, T. (2005). Measuring the True Benefit of Human Resources Outsourcing, *Workforce Management*, 84(7), 76-78.
- Holton, E. F. (1996). The flawed four-level evaluation model. *Human Resource Development Quarterly*, 7(1), 5-21.
- Horton, W. Evaluating the e-learning. *Training*, 42(9), 35-40.

- Jana, Reena (2006). On-the-job video gaming. *Business Week Online*, Retrieved May 15,2006, from http://www.businessweek.com/magazine/content/06_13/b3977062.htm
- Kane, C. M. (2005). Trends in IT outsourcing. *Association Management*, 57(9), 42-60.
- Kazmer M. & Haythornthwaite, C. (2004). Multiple perspectives on online learning. *SIGGROUP Bulletin*, 25(1), 7-11.
- Kim, K. J., Bonk, C. J., & Zeng, T. (2005). Research paper: surveying the future the workplace: e-learning: the rise of blending, interactivity, and authentic learning. *eLearn Magazine*, 2005(6), 2-6.
- Kirkpatrick, D. L. (1998). *Evaluating Training Programs*. San Francisco: Berrett-Koehler.
- Kirkpatrick, D. L. & Kirkpatrick, J. D. (2005). *Transferring Learning to Behavior*. San Francisco: Berrett-Koehler.
- Kirkpatrick, J. & Hawk, L. (2006). Curricula and evaluation: maximizing results. *T + D*, 60(6), 62-63.
- Kraiger, K., McLinden, D., & Casper, W. J. (2004). Collaborative planning for training impact. *Human Resource Management*, 43(4), 337-351.
- Krell, E. (2002, December). Calculating success: as companies struggle to evaluate their e-learning ROI, many are using different tools and metrics to measure results beyond T&E (travel and entertainment) savings. *Training*, 39(12), 46-51.
- Leedy, P. & Ormrod, J. (2001). *Practical Research Planning and Design* (7th ed.). Upper Saddle River, NJ: Merrill Prentice Hall.
- LeRouge, C. & Webb, H. (2003). Managing training in a technology context. *The ACM Special Interest Group on Management Information Systems (SIGMS '03)*, ACM Press: New York, NY, pp. 98-103.
- Mahapatra, R. & Lai, V. S. (2005). Evaluating end-user training programs. *Communications of the ACM*, 48(1), 67-70.
- Marlin, S. (2002, November). Class act: e-learning eclipses other technologies in delivering bottom-line results. *Bank Systems + Technology*, 39(11), 38-42.
- Martin, J. (2000). Roi: do it & prove it. *American Society for Training & Development*, Retrieved May 1, 2006, from www.astd.org/nr/exeres/7c131093-6f78-4694-98d9-e241be24d1d0.htm

- Mayberry, E. (2005). Kirkpatrick's level 3: improving the evaluation of e-learning. *Learning Circuits*, Retrieved September 26, 2006, from www.learningcircuits.org/2005/may2005/mayberry.htm
- Mayberry, E. (2007). Level 3 Assessments: Six Red Flags. *Learning Circuits*, Retrieved May 24, 2006, from <http://www.learningcircuits.org/2007/0307mayberry.html>
- Microsoft Corporation (2007, March). Strengthening American Competitiveness for the 21st Century. *Transcript of oral testimony by Bill Gates, Chairman, Microsoft Corporation United States Senate Committee on Health, Education, Labor, and Pensions*, Washington, D.C. Retrieved May 24, 2007, from <http://www.microsoft.com/Presspass/exec/billg/speeches/2007/03-07Senate.msp>
- Mitreanu, C. (2006). Is strategy a bad word? *MIT Sloan Management Review*, 47(2), 96-100.
- Montesino, M. U. (2002, Spring). Strategic alignment of training, transfer-enhancing behaviors, and training usage: a posttraining study. *Human Resource Development Quarterly*, 13(1), 89-108.
- Moran, J. (2002). ROI for e-learning. *Learning Circuits*, Retrieved May 15, 2006, from www.learningcircuits.org/2002/feb2002/moran.html
- Morrison, R. (2004). The success case method: find out quickly what's working and what's not. *Consulting to Management*, 15(3), 63.
- Mulgan, F. (2006). E-learning = environmental learning. *Learning Circuits*, Retrieved May 15, 2006, from www.learningcircuits.org/2006/april/mulgan.htm
- Mullich, J. (2004). A second act for e-learning: Part 1 of 2. *Workforce Management*, 83(2), 51-53.
- Mungania, P. (2003). The seven e-learning barriers facing employees. *The MASIE Center*, Retrieved January 12, 2006, from http://www.masie.com/researchgrants/2003/mungania_exec_summary.pdf
- Neubecker, R. (2004). How to measure the relationship between training and job performance. *Communications of the ACM*, 47(5), 63-67.
- Olfman, L., Bostrom, R. P. & Sein, M. K. (2003). A best-practice based model for information technology learning strategy formulation. *The ACM Special Interest Group on Management Information Systems (SIGMS '03)*, ACM Press: New York, NY, pp. 75-86.
- Overton, L. (2005). Reaching higher levels. *E.learning Age*, May(2005), 35-36.

- Paisittanand, S. & Olson, D. L. (2006). A simulation study of IT outsourcing in the credit card business. *European Journal of Operational Research*, 175(2), 1248-1261.
- Peterson, R. A. (1994). A meta-analysis of Cronbach's coefficient alpha. *Journal of Consumer Research*, 21(2), 381-391.
- Phillips, J., Phillips, P. P. & Zuniga, L. (2000). Evaluating the effectiveness and the return on investment of e-learning. *American Society for Training & Development*, Retrieved May 1, 2006, from http://www.astd.org/astd/Resources/eval_roi_community/return.htm
- Phillips, J. & Stone, R. D., (2003). *How to Measure Training Results. A Practical Guide to Tracking the Six Key Indicators*. New York: McGraw-Hill.
- Potter, J. (2000). Show me the money, in IT training! *ACM's Special Interest Group for University & College Computing Services*, Retrieved January 12, 2006, from <http://www.udel.edu/siguccs2000/FP/103-Potter.pdf>
- Purcell, A. (2000). 20/20 ROI. *American Society for Training & Development*, Retrieved May 1, 2006, from www.astd.org/astd/resources/eval_roi_community/2020.htm
- Pyzdek, T. (2004). Strategy deployment using balanced scorecards. *International Journal of Six Sigma and Competitive Advantage*, 1(11), 21-25.
- Reddy, A. (2002). E-learning ROI calculations: is a cost/benefit analysis a better approach? *E-learning*, 3(1), 30-32.
- Robinson, D. G. & Robinson, J. C. (2005). The strategic business partner model. *Training*, 42(5), 30-36.
- Robinson, D. G. & Robinson, J. C. (1989). *Training for Impact*. San Francisco: Jossey-Bass.
- Scott, G. M. (2005). Still not solved: the persistent problem of IT strategic planning. *Communications of the Association for Information Systems*. 2005(26), 1-10.
- Service, R. W. (2006). The development of strategic intelligence: a managerial perspective. *International Journal of Management*, 23(1), 61-70.
- Setaro, J. (2001). Many happy returns: calculating e-learning ROI. *Learning Circuits*, Retrieved May 1, 2006, from www.learningcircuits.org/2001/jun2001/elearn.html.

- Social engineering (security). (2007, June 26). In Wikipedia, The Free Encyclopedia. Retrieved June 26, 2007, from [http://en.wikipedia.org/w/index.php?title=social engineering %20security%29&oldid=140717555](http://en.wikipedia.org/w/index.php?title=social%20engineering%20security%29&oldid=140717555)
- Sloman, M. (2002). *The E-learning Revolution*. New York: AMACOM.
- Sugrue, B. & Rivera, R. J. (December, 2005). *ASTD 2005 State of the Industry Report*. ASTD Press.
- Taylor, C. R. (2001). E-Learning: the second wave. *Learning Circuits*, Retrieved May 15, 2006, from www.learningcircuits.org/2002/oct2002/taylor.html
- Trotter, A. (2002). California's online-learning potential evaluated. *Education Week*, 22(8), 11-12. 7
- Van Dam, N. (2003). *The E-learning Fieldbook*. New York: McGraw-Hill.
- Wang, G. & Li, G. (2003). Measuring HPT interventions: the dilemma, challenges, and solution. *Performance Improvement*, 42(10), 17-23.
- Webb, W. (2003). Enterprisewide speed limits: e-learning companies blame the economy for putting the brakes on enterprisewide training solutions, but customers point the finger at high costs, market confusion and murky ROI. *Training*, 40(1), 50-55.