



Mobile Phone Security Training

XYZ Corporation

By Team AAFL
Fall 2011 FDIT 705

Table of Contents

Problem Definition	3
Context	3
Statement of Problem	3
Source and Evidence.....	3
Scope Definition	3
Learner Analysis	4
General Characteristics	4
Entry Characteristics	4
Attitudinal and Motivation Characteristics:.....	4
Prior Experience.....	4
Common Errors Made By Novice Learners.....	4
Potential Audience Misconception	4
Learning Styles	5
Survey Questions.....	5
Context Analysis	6
Orienting Context.....	7
Insights into Organizational Politics	7
Instructional Context.....	7
Transfer Context	7
Collecting Data.....	7
Primary Data:.....	7
Secondary Data:	8
Task Analysis	8
Background	8
Prerequisites	9
Goals.....	9
Instructional Objectives	10
Instructional Approach	11
Prerequisites	11
System Requirements	11

Sequencing.....	11
Strategies.....	13
Time.....	13
Support.....	13
Instructional Materials	14
Formative and Summative Evaluation	14
Formative Evaluations	14
Connoisseur-Based Formative Evaluations with Experts	14
Data-Gathering Techniques	16
Small Group Formative Evaluations with Learners.....	16
Audience.....	16
Focus Questions	16
Resources.....	17
Data-Gathering Techniques	17
Sample Feedback Form and Sign-Off Sheet.....	17
Analysis.....	18
Reporting.....	18
Summative Evaluation with Learners	18
Analysis.....	19
Sample Feedback Form Questions	19
Projected Confirmative Evaluation	19
Appendix A: Regulatory Requirements for Security Awareness and Training	21
Appendix B: Partial Prototype	23
Project Approval	25

Problem Definition

Context

XYZ Corporation helps companies and agencies design, build, and maintain secure software through a variety of services. Services include best practices gap analysis, remediation services, and assessment services. Current and potential clients are in federal and private sectors in a very wide range of industries. Examples of XYZ's clients are Bank of America, Fidelity, Visa, Costco, Homeland Security, Sony Ericsson, and Coca-Cola. XYZ is an international company.

XYZ Corp. provides Information Technology (IT) Security Awareness training to its employees and contractors annually to meet identified needs: competitive advantage, compliance with applicable laws and regulations (see Appendix A), compliance with client contracts, and management of risks associated with loss of company assets and productivity. The company's current and potential clients are in a variety of industries and countries that also present additional requirements.

The current training consists of an eLearning course that contains all of the security practices that are required of the employee. Completion of the online course indicates the employee's agreement to comply with the security policies. The existing eLearning includes instructions for the learner on how to navigate the eLearning Course.

Laws and regulations for IT security include training employees and contractors on protecting information. Confidential information stored on, or accessible by, mobile phones is required to be protected.

Statement of Problem

XYZ Corp. is required to perform annual IT Security Awareness training to meet a variety of laws and regulations. Their current training does not include mobile phone security policies.

Source and Evidence

During an interview, the company's IT manager stated that the company has legal and contractual requirements to add mobile phone security training to their existing security awareness training. Additionally, he stated that, although they have not experienced a security breach due to the use of mobile phones, the company is proactive because they have to protect their reputation as a leader in an industry related to information security to maintain a competitive advantage.

Scope Definition

Needs for additional changes to the existing security awareness training were identified; however, this problem definition focuses on the addition of the mobile phone security policy.

Learner Analysis

General Characteristics

Primary audience (mandatory): All employees and contractors of XYZ Corporation. The total audience consists of 210 people. Employee demographics were obtained from XYZ Corp. Human Resources data:

- Age: 18-65 years old
- Gender: 70% male, 30% female
- Education range: High School Diploma, Bachelors, Masters, Ph.D.
- Work Experience: 1 week to 25+ years
- Reading level: All read at the 8th grade level or above

Entry Characteristics

- Basic mobile phone operations:
 - Send and receive phone calls
 - Send and receive text messages
 - Create and maintain a contact list
 - Send and receive e-mails
 - Configure device settings and features
- Read and write basic English
- Internet access and basic internet navigation skills

Attitudinal and Motivation Characteristics:

- Employees and contractors do not like having their mobile phones monitored. Some people view phones as personal and outside the preview of their employer.
- Employees/contractors and management recognize the importance of protecting confidential client and corporate data.

Prior Experience

- All employees and contractors have experience completing an online training course.
- All employees and contractors have been provided with a company Smartphone.
- All employees and contractors have some prior experience using a mobile phone.
- Although most employees and contractors know how to use their phones, only a few have knowledge of mobile security protocols (unless they received training from a former employer).

Common Errors Made By Novice Learners

- Employees and contractors do not know what types of information need to be protected on their mobile phones.

Potential Audience Misconception

- Employees and contractors may not think that they carry important information on their phone; therefore they may think they do not need to adhere to the company's IT Security rules and regulations.
- Only Smartphones need to be protected.

Learning Styles

One hundred employees and contractors were randomly selected to complete an electronic survey on how they learn best. Below are sample questions given to the survey participants to determine their learning styles. Learner responses were tallied after completion. If a participant scored mostly a's, they were identified with having a visual learning style. Those who scored mostly b's correspond with an auditory learning style, and those who scored mostly c's correspond with kinesthetic learning style.

Survey Questions¹

1. When you study for a test, would you rather:
 - a. Read notes, read headings in a book, and look at diagrams and illustration
 - b. Listen to a lecture given by a teacher
 - c. Play an interactive game

2. When you work at solving a problem do you:
 - a. Create a list, organize the steps, and check them off as they are completed
 - b. Read the problem out loud and consult others
 - c. Make a model of the problem or work through all the steps in your head

3. You have just entered a science museum, what will you do first?
 - a. Look around and find a map to see the locations and various exhibits
 - b. Talk to a museum guide and ask about the exhibits
 - c. Go into the first exhibit that catches your eye and read directions later

4. When you see the word "d-o-g", what do you do first?
 - a. Think of a picture of a particular cat
 - b. Say the word "d-o-g" to yourself
 - c. Sense the feeling of being with a cat (petting it, running with it, etc.)

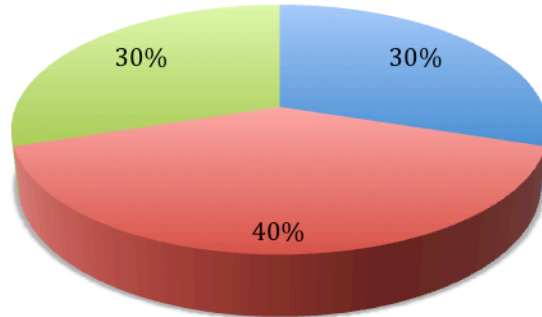
5. When you tell a story, would you rather
 - a. Write it
 - b. Tell it out loud
 - c. Act it out

They were also asked to choose their preferred learning environment and their preference between independent or group learning. The results are shown below:

¹ Source: University of South Dakota, B.W. James, <http://people.usd.edu/~bwjames/tut/learning-style/>, Adapted from Instructor Magazine, 8-89.

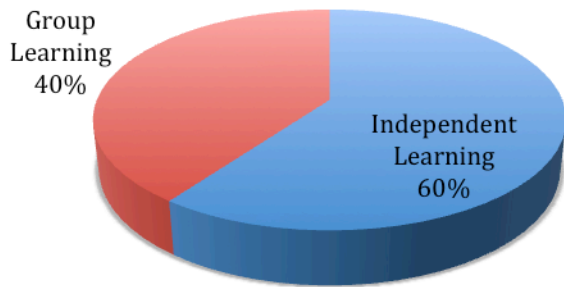
XYZ Corp. Employee Learning Styles

Auditory Visual Kinesthetic



- Auditory: 30%
- Visual: 40%
- Kinesthetic: 30%

XYZ Corp. Employee Preference on Learning Environment



Independent Learning Group Learning

- Prefer Independent Learning: 60%
- Prefer Group Learning: 40%

Context Analysis

Context analysis is a strategy for providing realistic information to provide rich instructional examples (Designing Effective Instruction, Morrison, pg. 474).

Orienting Context

Orienting context determines what goals the learners have for taking or attending the instruction, what the learners' perceived utility of the instruction and if the learners are accountable for mastering the content presented in the course (Designing Effective Instruction, Morrison, pg. 66)

XYZ Corp. provides an annual IT Security Awareness training to its employees and contractors to meet identified needs: competitive advantage, compliance with applicable laws and regulations, compliance with client contracts, and management of risks associated with loss of company assets and productivity. The current training consists of an eLearning course that contains all of the security practices that are required of the employee. Completion of the online course indicates the employee's agreement to comply with the security policies. We will be adding mobile security to this existing training content. By completing the IT Mobile Security Training, employees will be in compliance with legal and contractual requirements and keep company information secure.

Insights into Organizational Politics

- The culture prioritizes security-related issues.
- Managers support the training because it is a requirement by law.

Instructional Context

Instructional context considers the instructional environment (Designing Effective Instruction, Morrison, pg. 66).

Mobile Phone Security Training will be delivered online. Employees and contractors, on and off-site, will need computer and web access. The latest version of Java will also be required to support online training modules.

Transfer Context

Transfer context focuses on the application of the newly learned knowledge and skills (Designing Effective Instruction, Morrison, pg. 68).

Supervisory teams of all departments will implement new policies among their employees for future projects. Supervisory personnel will monitor their staff by requiring all members of the organization, with a company Smartphone to provide an annual updated training certificate (which will automatically be provided once the learner successfully completes the online training course) reflecting the completion of the most recent version of the online course. The certificate will represent the learner's knowledge of the Mobile Security content and their agreement to comply with the regulations mentioned during the training.

Collecting Data

Primary Data:

- Demographics were obtained from the corporate HR department.
- A random survey consisting of open and closed ended questions was distributed randomly to 100 members of the organization (employees, contractors, and seasonal interns) to

determine the audience learning styles, preferences on independent and group learning, and preferred learning environments.

- Interviews were conducted to gain insight on learner attitudes, motivation, and organization culture.
- Interviews and surveys were used to determine the prior experience levels of the audience.
- The IT department provided information on the phones provided to employees.

Secondary Data:

- According to the National Institute for Standards in Technology (NIST) Report: Guidelines on Cell Phone and PDA Security:
“Cell phones and personal digital assistants (PDAs) have become indispensable tools for today’s highly mobile workforce. Small and relatively inexpensive, these devices can be used for many functions, including sending and receiving electronic mail, storing documents, delivering presentations, and remotely accessing data. While these devices provide productivity benefits, they also pose new risks to organizations.”

Task Analysis

The task analysis is a collection of procedures for identifying and describing topics related to a goal or need (Designing Effective Instruction, Morrison, pg. 476).

Background

XYZ Corp. is adding mobile phone security to their existing IT Security Awareness training. This training is mandated by law (see Appendix A) and enforced by the company’s IT board. The company currently provides all employees and contractors with an online course that is linked to the companies Learning Management System. This IT Security Awareness training is updated annually, and contains all of their IT security standards. Employees and contractors are required to complete the online quiz at the end of the course, indicating they have read and understand the standards of the companies IT Security policies.

Employees and contractors have company issued mobile phones. This training will apply to any phone that an employee uses for work or possesses at work.

Areas of concern for mobile phone security that are used for a task analysis and training outline are derived from *Guidelines on Cell Phone and PDA Security*, National Institute of Standards and Technology (NIST), US Department of Commerce, October 2008 and TechTarget’s website (<http://searchmobilecomputing.techtarget.com/feature/Mobile-security-policies#define>).

According to the IT Manager, the company’s IT board endorses the use of these guidelines.

This task analysis uses a topic analysis approach because the focus of the training is the company’s policies (rules and procedures). Learners will need to familiarize themselves with the policies, in order to apply the policies to workplace scenarios and successfully complete the IT Mobile Phone Security unit of the IT Security training.

General IT security concepts, such as defining sensitive data, are covered in the existing IT security training. Also excluded from this training are operational steps that are specific to specific types of phones. Employees and contractors are referred to their cell carrier or the IT help desk for operational assistance specific to their devices.

Prerequisites

- **Basic mobile phone operations:**
 - Send and receive phone calls
 - Send and receive text messages
 - Create and maintain a contact list
 - Send and receive e-mails by mobile phone (if available)
 - Contacting carrier for additional help
 - Advanced mobile phone operations:
 - Add and remove applications (if available)
 - Change settings (i.e. encryption, passwords)
- Read and write basic English
- Know how to access the company's LMS and navigate the LMS
- Know how to contact the IT help desk

Goals

The purpose of this training is to provide the company's policies on mobile phone security. The mobile phone security policies will consist of three topic areas: Device Security, Information Security, and Network Security.

Employees will be able to recognize and agree to the following:

I. Device Security

1. **Secure Mobile Device**
 - a. Mobile phone users must have mobile phone secured at all times
 - i. Phone should never be unattended
 - ii. Do not leave phone in the care of others
 - iii. Store in locked cabinet or drawer
 - iv. Leave phone at home when you do not need it
2. **Enable non-cellular wireless interfaces only when needed**
 - a. Mobile phone user should Turn off Bluetooth, Wi-Fi, infrared, and other wireless interfaces until they are needed
 - i. Staying off-line avoid malicious infections
3. **Avoid questionable actions that would lead to a mobile security breach**
 - a. Mobile user must read permissions before installing apps. Some apps are open and vulnerable to attacks.
 - b. User should avoid downloading material from an unknown source.
4. **Report and deactivate compromised devices**
 - a. A mobile phone user must report a device that has been compromised (lost, stolen, or tampered with)
 - i. Call IT help desk
 - ii. Verify user authentication

- iii. Follow prompts from help desk

II. Information Security

1. Reduce exposure of sensitive data
 - a. Mobile phone users should avoid storing sensitive data on a mobile device if it is not necessary
 - i. If the presence of sensitive data is not avoidable, the data should be encrypted until required
 - ii. If a phone does not provide encryption user must contact the IT help desk for third party encryption software
 - b. Any messages or contacts received on a mobile phone from an unknown number or device should be treated with suspicion.
 - i. Messages should be destroyed without opening and connections denied.
2. Back up data
 - a. Mobile users must use phone carrier back up service or manually back up their phone to their company-issued laptop monthly
 - b. Users should not back up to a memory card since memory cards are often stored with phones

III. Network Security

1. Employ user authentication, content encryption, and other available security facilities
 - a. All functions of the mobile device, except emergency calls, should be password protected
 - b. All passwords must be considered a strong password (Organization policy regarding the length and composition of passwords and PINs for cell phones: at least eight characters including at least one capital character and one symbol.)
 - c. Employee/Contractor should not set phone password to be the same as a password used for network access or access to other devices and applications
 - d. A phone user must turn on timeout feature to lock the phone after three minutes of inactivity
 - e. A mobile phone user must encrypt sensitive data

Instructional Objectives

Instructional objectives are statements describing what the learner is specifically required to learn relative to a topic (Designing Effective Instruction, Morrison, pg. 475).

Participants will be able to:

- Identify how to secure their mobile phones at all times
- Recognize instances when wireless interfaces are not needed
- Recognize questionable actions that would lead to a mobile security breach
- Identify good back-up habits
- Identify a compromised device

- Identify the steps for reporting a compromised devices
- Identify suspicious content
- Identify the steps for properly discriminating against suspicious content
- Recall proper ways of storing sensitive data on a mobile device
- Identify organization policy regarding strong passwords or pins
- Recognize when encryption should be implemented

Instructional Approach

Instructional approach includes the decision on the general learning environment (delivery strategy) and the sequences and methods of instruction for achieving the objectives (Designing Effective Instruction, Morrison, pg. 150).

Prerequisites

- Basic mobile phone operations:
 - Send and receive phone calls
 - Send and receive text messages
 - Create and maintain a contact list
 - Send and receive e-mails by mobile phone (if available)
 - Contacting carrier for additional help
 - Advanced mobile phone operations:
 - Add and remove applications (if available)
 - Change settings (i.e. encryption, passwords)
- Read and write basic English
- Know how to access and navigate the company's Learning Management System (LMS)
- Know how to contact the IT help desk

System Requirements

- Internet access
- Updated Java software
- Standard browser (Internet Explorer, Firefox, Chrome or Safari)
- LMS access

Sequencing

Sequencing is the efficient ordering of content in such a way as to help the learner achieve the objectives (Designing Effective Instruction, Morrison, pg. 136).

The Mobile Phone Security Training unit will consist of an overview module, three instructional modules (*Device Security, Information Security, and Network Security*) and a unit completion/test module. The overview and test modules (first and last modules) are ordered by concept-related sequencing (class relations phenomena). The three instructional modules are sequenced using world-related sequencing (by physical phenomena).

IT Mobile Phone Security Unit

Module	Objectives and Strategies
<p>Module I: <i>Unit Overview</i></p>	<p>Participants will be able to:</p> <ul style="list-style-type: none"> • Be familiar with the objectives of the unit through a brief listing of objectives • Be familiar with the organization and content of the training through a brief topical outline <p>Strategy:</p> <ul style="list-style-type: none"> • Present a list of objectives for all modules
<p>Module II: <i>Device Security</i></p>	<p>Participants will be able to:</p> <ul style="list-style-type: none"> • Identify how to secure their mobile phones at all times • Recognize instances when wireless interfaces are not needed • Recognize questionable actions that would lead to a mobile security breach • Identify good back-up habits • Identify a compromised device • Identify the steps for reporting a compromised devices <p>Strategy:</p> <ul style="list-style-type: none"> • Scenario-based knowledge check with automated feedback to verify understanding of the objectives
<p>Module III: <i>Information Security</i></p>	<p>Participants will be able to:</p> <ul style="list-style-type: none"> • Identify suspicious content • Identify the steps for properly discriminating against suspicious content • Recall proper ways of storing sensitive data on a mobile device <p>Strategy:</p> <ul style="list-style-type: none"> • Scenario-based knowledge check with automated feedback to verify understanding of the objectives
<p>Module IV: <i>Network Security</i></p>	<p>Participants will be able to:</p> <ul style="list-style-type: none"> • Identify organization policy regarding strong passwords or pins • Recognize when encryption should be implemented <p>Strategy:</p> <ul style="list-style-type: none"> • Scenario-based knowledge check with automated feedback

	to verify understanding of the objectives
Module V: Course Completion	<p>Participants will:</p> <ul style="list-style-type: none"> • Demonstrate understanding of the content through a 15-question quiz that they must obtain at least a score of 80%. The quiz will be divided into three parts where five questions will reflect content from each module. • Pass the exam and receive a certificate, which is linked to the learning management system or be given an opportunity to review the unit and retake the exam.

Strategies

The following methods will be employed in the training unit.

Method	Use of Method
Presentation	<p>Each module of the Mobile Phone Security Training unit will contain slides, narration, and visual cues.</p> <p>The presentation will contain:</p> <ul style="list-style-type: none"> • An overview explaining new security policies • Different situations where the application of various laws or policies is relevant • Related scenario-based exercises <ul style="list-style-type: none"> – Allow participants to apply new knowledge from presentations by presenting them with four options from which they must choose a correct action or policy – Reinforce content through the scenario-based knowledge check with automated feedback to verify understanding of the objectives – All response options will provide feedback explaining why a particular option is correct or incorrect
Application	<p>The course will incorporate realistic business situations as much as possible to ease the transfer of application from the learning environment to the work environment through scenario-based exercises.</p>

Time

The participants are given the opportunity to go through the modules at their own pace.

Support

A training administrator will respond to questions and requests for assistance sent to the training support email address (training@xyz.com).

Instructional Materials

The instructional materials for the Mobile Phone Security Training unit will consist of:

- An online tutorial created in Adobe Captivate. The interface of the online tutorial will consist of a unit overview module, a device security module, an information security module, a network security module, and a quiz module. The modules will include text, audio narration, and images to compliment concepts and illustrate workplace scenarios.
- Feedback that will be linked to the Knowledge Check questions. The Knowledge Check questions are designed to test the learner's comprehension of the content for each section (device security, information security, and network security). Learners will be provided with a workplace scenario and then asked a question pertaining to the module. The feedback will provide learners with information on why the answer that they chose was correct or why the answer that they chose was incorrect. If the employees answer incorrectly, they will have the option to go back and review the training materials again. If the employee does not pass the quiz at the end of the course, they will be prompted to review the modules and retake the quiz.
- A Microsoft PowerPoint presentation and PDF version of the eLearning pages and narration script will be embedded in the online unit for learners to print off for notes.
- An online unit incorporating hypermedia links to the official sites where the security policies are listed. The links will be "learner controlled," meaning that learners will not be required to visit these sites.
- A certificate of completion will be provided to users once they have successfully completed the online Mobile Phone Security unit by passing the quiz at the end of the training.

Formative and Summative Evaluation

Evaluation of the Mobile Phone Security Training unit includes formative, summative, and confirmative approaches. All three types of evaluation include multiple data sources. The overall goal of evaluation is to determine student success in learning. Evaluation results will be used to improve how the course is taught.

Formative Evaluations

Formative evaluations test a new instructional program with a sampling of learners during the design and development phase and use the results to improve the program's front-end analysis (Designing Effective Instruction, Morrison, pg. 474). The formative evaluation for this training consists of connoisseur-based (expert-based) and small group evaluations.

Connoisseur-Based Formative Evaluations with Experts

Connoisseur-based evaluations are used to identify obvious problems with processes and products. Connoisseur-based reviews will be conducted with 15 instructional design colleagues and the IT Manager, who serves as the subject matter expert (SME), after each of the following phases of instructional design and focused on the areas identified below. There will be times budgeted in advance for these reviews to take place. Revisions will be made based on results prior to moving on to the next phase.

Instructional Design Phase	Evaluation Areas	Mapping to Content
Instructional Problem Definition	<ul style="list-style-type: none"> • Is the problem correctly identified? • Is this problem best addressed by an instructional intervention? 	<ul style="list-style-type: none"> • Overview Module
Learner/Context Analysis	<ul style="list-style-type: none"> • Confirm identification of the correct target audience. • Confirm identification of how the audience characteristics and environment characteristics can provide opportunities or limitations to the design. 	
Task Analysis	<ul style="list-style-type: none"> • Is the Task Analysis thorough and accurate? • Will the content and skills identified alleviate the instructional problem? 	<ul style="list-style-type: none"> • Module Structure
Instructional Objectives and Sequencing	<ul style="list-style-type: none"> • Is each objective complete, concise, and adequately describe the intended outcome? • Are objective in alignment with the task analysis and goals? • Do the objectives support the achievement of the goals and alleviation of the problem? • Does each objective communicate the intended outcomes? <ul style="list-style-type: none"> ○ Does each objective include the needed parts (i.e., verb and content)? ○ Is each objective measureable? • Does the task analysis include the required information for the sequencing strategy? 	<ul style="list-style-type: none"> • Device Security Module • Information Security Module • Network Security Module
Instructional Approach and Message	<ul style="list-style-type: none"> • Comparing the strategies against the objective, does the instruction develop the appropriate knowledge and skills? • Do the objectives, content, and instructional strategies address the instructional problem? • Is the logic of the sequencing still appropriate after designing the instructional strategies? • Does the pre-instructional strategy selected represent the best fit between learners and instruction? • Message design is appropriate? <ul style="list-style-type: none"> ○ Illustrations accurately illustrate the instruction. ○ Illustrations are legible when reproduced. 	<ul style="list-style-type: none"> • Device Security Module • Information Security Module • Network Security Module

	<ul style="list-style-type: none"> ○ Copyright clearance is obtained (if needed). ○ Text structures are identified with appropriate signal words to alert the learners. ○ Do headings convey the structure of the text? <ul style="list-style-type: none"> ▪ Can the reader easily identify the different headings? ▪ Are the headings distinct from one another and from the text? 	
Instructional Materials Concepts	<ul style="list-style-type: none"> • Unnecessary cognitive load is not created through poor designs that create a split-attention effect or redundancy. • Text and graphics reduce cognitive load. • Materials are supportive of the objectives. • Materials are presented in a concrete manner. • Initial presentation and generative strategy are implemented for each objective. 	<ul style="list-style-type: none"> • All Modules

Source: *Designing Effective Instruction*, Morrison, Ross, Kalman, Kemp, 2011.

Data-Gathering Techniques

Evaluators will be provided with verbal and written presentations of the design products as they are completed (after each of the above phases) and requested to complete online feedback forms covering the above evaluation areas.

Small Group Formative Evaluations with Learners

Following the design of instructional materials concepts and completion of revisions resulting from the connoisseur-based evaluations, a prototype will be developed and used as a basis for small group formative evaluations to confirm that the methods meet the instructional goals and objectives.

Audience

Evaluators are chosen to represent a range of skills. They include 10 employees: two senior managers, two IT help desk employees, three mid-level managers, and three interns.

Focus Questions

The small group formative evaluation will focus on the following questions based on the prototype:

- Does the instruction properly address the problem definition, goals, and objectives?
- Are the scenarios engaging?
- Do the scenario examples reinforce the mobile phone security policies presented?
- Are the modules arranged in the proper order?
- Was the course organized to allow for navigational ease?
- Overall, was the presentation too lengthy?

Resources

Materials include the prototype eLearning unit, draft tests, observer’s checklists, evaluator’s notes, a conference room, and computer equipment for four hours.

Data-Gathering Techniques

Participants will be instructed to complete the eLearning unit and an anonymous feedback form independently and provide their reactions based on their experiences regarding the overall structure, organization, sequence, and timing at the end of the course.

Sample Feedback Form and Sign-Off Sheet

This is an example of the anonymous feedback form evaluators will receive during the small group evaluation:

Questions	Yes	No	Comments
Is the course goal stated accurately?			
Were the modules in an appropriate order?			
Does each module appropriately reflect learner objectives?			
Overall, was the course easy to navigate?			
Were the scenario-based questions appropriate for this course?			
Is the final quiz a good assessment of the course?			
Did you find the length of course too long?			

Instructional designers will observe and note participant reactions through scenario exercises and the final assessment. Automatic score reporting and analysis is completed through the company’s learning management system and sent to the ID team.

Project Sign-Off		
Review	Evaluations for Revisions	Signatures
Primary Review Date: _____	___ Comments for revisions indicated in feedback form. ___ No additional revisions. Course design accepted.	IT Manager: _____
Final Review Date: _____	___ Comments for revisions indicated in feedback form. ___ No additional revisions. Course design accepted.	IT Manager: _____

Analysis

The ID team will compile scores, observation notes, and feedback for modifying the instructional materials. Evaluation instruments are also evaluated and corrected for clarity and effectiveness for use in summative evaluations that follow.

Reporting

After the small group formative evaluation, the ID team will compile learner quiz results, observations, and feedback into an official summary. Success criteria is 100% of learners obtaining 80% or higher to the unit quiz. The report will review the overall effectiveness of the course materials and strategy used. The report will be emailed to the IT Manager within three business days along with suggested changes to the course and test material. The online course for Mobile Phone Security Training will be implemented once approved by the IT Manager.

Summative Evaluation with Learners

Summative evaluations measure how well the major outcomes of a course or program are attained at the conclusion of instruction (posttest) or thereafter on the job (Designing Effective Instruction, Morrison, pg. 476).

The summative evaluation of this training will occur following the completion of revisions resulting from the small group formative evaluation and launch of the training. It will include quiz results and learner reactions. Learners will be instructed via email to complete the eLearning unit and an online feedback form independently.

Analysis

The summative evaluation will include quiz and feedback data collected over three months following launch of the training.

Automatic score reporting and analysis of feedback will be completed through the company's learning management system and sent to the ID team.

Quiz scores will be displayed as frequency distributions to help illustrate any testing trends. Quiz scores will be represented by a histogram and an individual question analysis can be applied to determine if the material is covered insufficiently for an individual subject or overall.

Sample Feedback Form Questions

This is an example of the anonymous feedback form learners will receive:

Questions	Yes	No	Comments
Is the course goal stated accurately?			
Were the modules in an appropriate order?			
Does each module appropriately reflect learner objectives?			
Overall, was the course easy to navigate?			
Were the scenario-based questions appropriate for this course?			
Is the final quiz a good assessment of the course?			
Did you find the length of course too long?			

Projected Confirmative Evaluation

Confirmative evaluation is a continuous form of evaluation that follows the summative evaluation. The confirmative used to determine whether a course is still effective (Designing Effective Instruction, Morrison, pg. 473).

The ID team will conduct a series of six checks on completion statuses throughout the year prior to the compliance training deadline. Success criteria is 100% of learners obtaining 80% or higher on the unit quiz.

Twelve months after the Mobile Phone Security Training has been implemented, the Instructional Design team will request IT department data on mobile security phone violations. Another request for data will be placed six months later to compare whether violation cases have decreased by 75%. Additionally, the ID team recommends that Kirkpatrick level five Confirmative Evaluations be completed. They would be based on five criteria levels: Reaction, Learning, Behavior, Results, and Return on Investment (ROI).

Appendix A: Regulatory Requirements for Security Awareness and Training

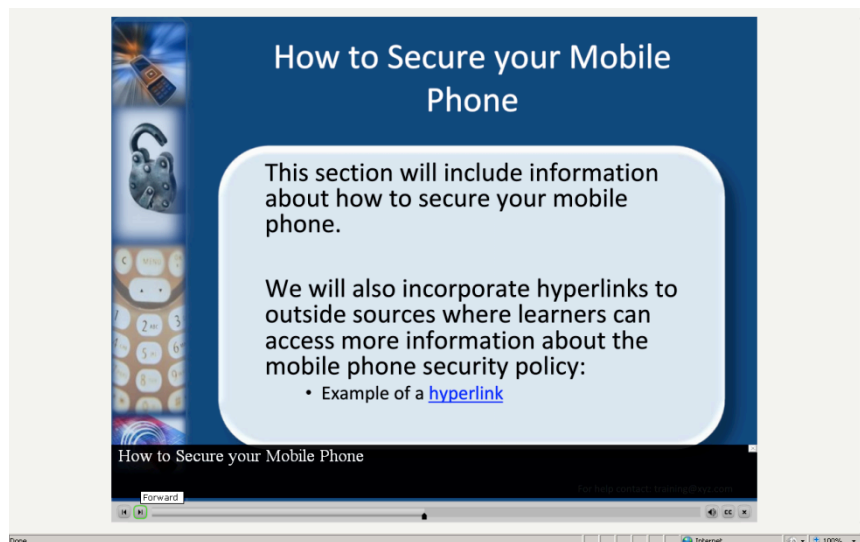
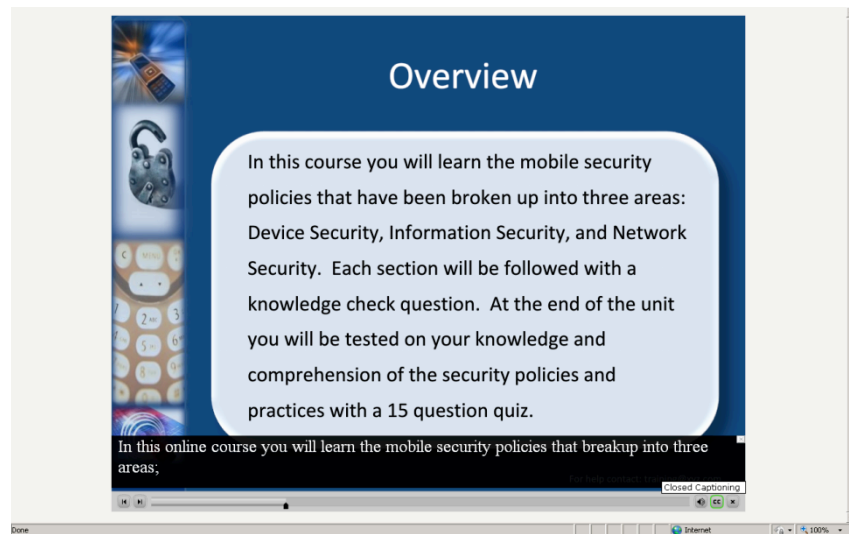
Regulation/Framework	Industry/Country	Awareness/Training Requirement
HIPAA (Health Insurance Portability and Accountability Act of 1996)	Healthcare (U.S.)	Security Final Rule 164.308 (a)(5)(i) (R) Implement a security awareness and training program for all members of its workforce (including management).
ISO/IEC 17799:2005 Section 8.2.2 Information security awareness, education, and training	Security Framework (International)	All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
Sarbanes-Oxley Act, Section 404 Based on COBIT™ (Control Objectives for Information Technology)	All Publicly Traded Companies (U.S)	DS 7.2 Delivery of Training and Education Appoint trainers and organise training sessions on a timely basis. Registration attendance and performance evaluations should be recorded.
Chemical Sector Cyber Security Program	Chemical Sector (U.S.)	5.15 Staff Training and Security Awareness Effective cyber security training and security awareness programs should provide each employee with the information necessary to identify, review and remediate control exposures.
Gramm-Leach-Bliley Act (GLBA) Title V - Section 501	Financial Services (U.S.)	Safeguards Rule 314.4: “ (b) Identify reasonably foreseeable internal and external risks [] including - (1) Employee training and management.”
FERC Cyber Security Standard CIP-004-1: Personnel & Training	Energy/Infrastructure (U.S.)	"R1. Awareness - The Responsible Entity shall establish, maintain, and document a security awareness program. The program shall include security awareness reinforcement on at least a quarterly basis"
Federal Information Security Management Act (FISMA) NIST SP 800-26	Federal Government (U.S.)	“(a) The head of each [Federal] agency shall (4) Establish security awareness training to inform all personnel, including contractors and other users of information systems of (a) Determining the risks associated with their activities, and (b) knowing their responsibilities in complying with agency policies and procedures designed to reduce these risks; ”
PIPEDA (Bill C6) - Personal Information Protection and	All Industries (Canada)	Principle 4.1.4 - Organizations shall implement policies and practices to give effect to the principles, including [...] (c) Training staff and communicating to

Electronic Document Act		staff information about the organizations policies and practices.
-------------------------	--	---

Source: <http://www.informationshield.com/security-awareness-requirements.html>

Appendix B: Partial Prototype



The images below are screenshots taken from the prototype. The slides were created using PowerPoint and Adobe Captivate. The screenshots demonstrate the content and navigational layout. The resources slide shows how hyperlinks will be included in the project for additional information for the learner. The quiz slide demonstrates how feedback will be used to guide the learner on how to receive the correct information in order to successfully complete the unit and receive credit for the compliance training.



Knowledge Check

The knowledge check sections will include workplace scenarios where the characters involved will be faced with a mobile phone security issue.

Learners will be expected to apply what they have learned in the previous slides to determine what should be done to successfully handle the situation and be in compliance with the mobile phone security policy.



Knowledge Check

Forward

Resources

training@xyz.com

[PDF of Mobile Phone Security Unit](#)

[PowerPoint of Mobile Phone Security Unit](#)

For help contact: training@xyz.com

Quiz

True or False? You should lock up your mobile device when it is unattended.

A) True
 B) False

Correct - The answer is A) True. According to policy xxx, you are required to keep your mobile phone locked when it is unattended. For further information review the Device Security module. Click anywhere or press 'y' to continue.

Clear Back Submit

Project Approval

I have reviewed and approved the design plans for the Mobile Phone Security Training unit, with changes, additions, deletions or corrections as annotated in the instructional design document.

I hereby give you approval to proceed with creating the drafts of all course materials. I also give my approval for you to invoice my department for satisfactory completion of the design plans of this project.

I understand that further changes to the structure, objectives or content of the unit will likely result in a delay in the final delivery date and could result to additional costs.

IT Board Chair

Date