Awareness and Accountability in Information Security Training

By Michael Mellor and Daniel Noyes

Abstract

Basic information assurance threat awareness must be raised through training that establishes individual accountability. While a great deal of research has been performed in regard to information assurance training, the authors provide evidence that supports the argument that adding personal accountability into the training process can play a valuable role in increasing the overall strength of the human factor in information security.

Introduction

"Amateurs hack systems, professionals hack people" (Schneier 2000). Basic information assurance threat awareness must be raised through training that establishes individual accountability. The traditional corporate training sessions are known to be long, tedious, and boring where very little if any learning occurs (Coverstone 2003). Information assurance topics are typically thought of as 'techie' topics that are tuned out by the general population (Desman 2003). The frequency of occurrences in users remaining susceptible to phishing, password problems, internet usage abuse, social engineering, and others (CSI/FBI Computer Crime and Security Survey 2005) are evidence of a growing problem and illustrate the need for more effective user training. This legacy training process erroneously transforms the given organizations largest asset into an equally large liability (Bradford 2003).

Great strides have been made to change these ineffective legacy training systems into modern up-to-date effective programs (Bradford 2003). Despite these great strides, implementation seems to be difficult. (Desman 2003) We have used the National Institute of Standards and Technology (NIST) special publication 800-16 to create a baseline security training and assessment instrument which we believe will develop greater awareness and individual accountability in the end user.

In terms of this paper, individual accountability represents taking ownership of something and understanding the consequences pertaining thereto. When this is added to a training program, it literally transforms the trainee from a passive learner to an active learner as they become individually accountable for the material presented.

The training that we developed is intended to be interactive where the participant demonstrates knowledge learned and certifies competency in all areas presented. The trainer also certifies that the participant is competent in all areas presented, which adds an additional layer of accountability. This process promotes active learning as both the participant and the trainer have an active stake in assuring that the presented knowledge is understood.

The training is presented as a process that needs to be customized by individual organizational needs. The scope of this paper is to present a baseline instrument for organizations to use as a reference in

developing their own training programs. What we developed is a rudimentary version of this baseline training and assessment instrument which can be used by any organization as a reference tool.

As we developed this training process, we used a leading government standard as a point of reference. The NIST SP800-16 defines five phases that training programs must go through in order to provide a rich learning environment. They are needs analysis, goal formation design, development, implementation, and evaluation. This established method has been used in the development of countless training programs (Pfefer 2003). This paper will discuss the process that we followed as we developed this training and assessment instrument using the five phases of a successful training program.

Any knowledgeable security professional will tell you that technology is not a panacea. When it comes to protecting information, people, or the human factor, are the most critical link in assuring information. Without proper training, passwords such as "Idaho" may be all that stands between a company's information and an attacker.

Background

Information Security is typically thought of as technical controls and countermeasures that only have small areas that actually pertain to people (Desman 2003). We propose however that people are the most valuable asset and can also prove to be the largest liability. In this study we argue that basic information assurance training can be provided to employees through low cost methods that have high learning retention yields.

This project originated after meetings with human resource directors at multiple locations. Checklists were always presented covering basic aspects of the business including where paychecks are to be picked up at, acceptable behavior, summary of benefits, etc. A checklist was always used where the trainer would certify that each area was covered that pertained to employment at the given establishment. This method transforms the trainer as well as the trainee into equal stakeholders through increasing individual accountability.

We recognized that a similar procedure might be useful for introducing new employees to organizational security policies and practices. That is, employees could be given a simple training course in that first contact with human resource or personnel workers. The checklist is used to certify that the trainee is exposed to and gains acceptable proficiency in each of the ten information security domains.

While we do assert that the proposed training instrument will play an important part in the overall process of training employees, it is only a small piece in a large and complicated process.

Development of Baseline Security Training and Assessment Instrument

The proposed ten domains are passwords, social engineering, email, physical security, locking or logging off your computer, unauthorized programs, handling confidential data and material, internet usage, phishing, and handling storage media and portable computers (NW3C & FBI, 2005) (ISO 17799) (Schell & Martin 2004).

We developed this baseline training and assessment instrument to cover these ten domains. Included in this instrument are a test, a training outline, a checklist, and a sheet of reminders. The test helps gauge the level of security awareness held by employees. The training outline helps in effective delivery of the training material by providing more in-depth information about the ten domains. The checklist is a key part of the training process. It is used as a record which certifies that the trainee was

exposed to and demonstrated an acceptable level of proficiency in each of the ten security domains. The reminder sheet is kept by all participants to be used as a reference or reminder of the training completed.

Although we were able to support our rationale for using the domains we selected and the training instrument we created, we wanted to find out if what we assumed about these issues in the business world was actually correct. Armed with our four newly created training tools, we decided to conduct a minimal survey of local businesses and see how they compared with our assumptions. We agreed that the financial industry would be a proper target for our survey as they deal with sensitive information and use technology every day in performing their duties. The process we followed was only a portion of what a company should expect to do, yet it yielded great results.

Organizations may need to take the training and assessment instrument and change it to match their organizational needs. Implementations of this instrument can be as simple as a piece of paper that both the employee and trainer sign (see checklist) or as complicated as a computer assisted training program. A computer assisted training program could be used to track employee progress and report to management on employee progression. This would ease the workload associated with the training as well as automate the overall process (Dagada 2004).

In the Information Systems Security journal, Susan Hansche in her paper "Information System Security Training: Making it Happen", defines training as "more formal and interactive than an awareness program. It is directed toward building knowledge, skills, and abilities that facilitate job capabilities and performance. The days of long, - and dare one say boring – lectures have been replaced with interactive and meaningful training (Hansche 2001)." The success of any given training program is vitally dependent on the designers implementing it to fit organizational needs and at the same time providing a rich learning environment for the participants.

The NIST SP800-16 defines five phases that training programs should go through to fulfill the goals of customization and to provide a rich learning environment. They are: needs analysis, goal formation design, development, implementation, and evaluation (NIST SP800-16). A basic synopsis of each phase as well as the process that our training instrument underwent is explained below.

Needs analysis

During the needs analysis phase it is important for the organization to make an honest assessment of what the participants already know and what awareness is required. We knew that during our testing process organizations were going to be very hesitant about providing us with in depth information regarding their employee weaknesses. With this in mind we found ten areas where virtually all businesses had reported problems and we used that as a basis for our checklist. Our checklist containing the ten domains is presented as ten areas where the 'average' employee might lack knowledge.

An administered test provides a valuable resource in the needs analysis phase. It will provide instructors with a good idea on where participants already have satisfactory competency and areas where additional instruction is required.

The pre-test will more than likely uncover several areas where participants lack an understanding of basic information assurance knowledge or procedures. The next step is to prioritize the information that needs to be presented during the training program (Moore 2003). Possible prioritization factors can include:

- Legal requirements
- Cost-effectiveness
- Management pressure
- The organization's vulnerabilities

- Threats, information sensitivity, and risks
- The makeup participant population (Hahsche 2003)

Our needs analysis phase mainly consisted of research into areas where the majority of businesses were seeing the most problems. We then prioritized our training based on the priority of the threats as well as the legal requirements associated with the given threats. After having established this solid foundation, we went about setting goals that would direct the remaining aspects of the training program.

Goal formation design

In order for any training program to be successful, goals must be set at the initiation of the training program. These goals are driving forces in accomplishing the training objectives. In establishing goals, priorities of the organization must be taken into account as realistic goals drive the training program forward.

During the establishment of goals, it is also very helpful to define the material that is being presented to the audience. Peltier, in his "Implementing an Information Security Awareness Program" article defines five key elements that must be presented to the audience including:

- A process to take the message to the user community to reinforce the concept that information security is an important part of the business process
- Identification of the individuals who are responsible for the implementation of the security program
- The ability to determine the sensitivity of information and the criticality of applications, systems and business processes
- The business reasons why basic security concepts such as separation of duties, need-to-know, and least privilege must be implemented
- That senior management supports the goals and objectives of the information security program (Hahsche 2003)

During the early needs analysis and goal formation design these five key elements need to be considered and factored into the planning of the training. A key component is also for participants to understand that management is fully behind and supports the given training program (Peltier 2005). A great deal of the individual accountability factor is dependent upon management fully supporting the training.

Convincing senior management that the training is essential to the growth and integrity of the organization is vital. If senior management perceives the training as unimportant, this mindset will more than likely be passed on to the participants. Susan Hansche, in her article "Information System Security Training: Making it Happen" outlines some important points to help secure the support of senior management:

- Training helps employee retention
- Find an ally in senior management to be an advocate
- Make sure the training program reflects the organization need
- Market the training program to all employees
- Start small and create a success
- Discover management's objectives (Hansche 2003)

Presenting each of these points to senior management is essential. As senior management catches the vision of the training program and fully supports it, the results of the training will be greatly enhanced. In order for the training to be successful we knew that senior management needed to be on board with the idea of training their employees. After presenting the above points and demonstrating

the training to the managers they became enthusiastic and were eager to begin. This step was vital in establishing the individual accountability in participants that this training requires.

As we designed the proposed training tool our goals were to improve information security awareness among participants as well as to raise the feeling of personal accountability in participants. These goals were the foundation of all training material that was prepared as well as being the driving force behind the entire process.

Development

The NIST 800-50 defines two questions that must be asked during the development phase:

- "What behavior do we want to reinforce?" – awareness
- "What skill or skills do we want the audience to learn and apply?" – training (NIST 800-50)

One of the core goals of the training program is to ensure that participants learn and retain as much information as possible. Thomas Peltier defines three major learning types:

- Auditory. These people must hear something in order to grasp it
- Mechanical. This learning-type must write down the element to be learned. Those taking notes during meetings are typically mechanical learners
- Visual. This type of learning, of which 90 percent of our audience is, need to see a picture or diagram to understand what is being discussed. People who learn via this method normally have whiteboards in their offices and use them (Peltier 2005)

In formulating the training instrument we researched major information security issues that businesses faced as well as the human learning process (NIST 800-50). We also attempted to provide enrichment at every level for each learning type. It is important for the instructor to make note of individual learning styles where possible and to tailor the training to specific learning styles.

Implementation

Implementation is one of the more important phases of the entire training process. The implementation phase is where the rubber meets the road, so to speak. All of the planning that has been performed finally becomes realized. Regardless of flawless execution leading up to this point, without a successful implementation the training will be a failure.

A format must be decided upon in this stage for presenting the training material. The training process can be presented as a simple checklist on paper or as complex as a computer assisted training program. A vital aspect is to decide on the best method to meet the learning objectives, the number of students, and the organization's ability to efficiently deliver the instructional material (Hansche 2001). This requires an assessment of the organizational resources that are available to dedicate to the training program.

The majority of organizations are constantly performing some kind of training. It is a good idea to find out what organizations have done in the past and what has been both successful and unsuccessful. It is important that the training matches the culture and atmosphere of the company. Speaking with management that has conducted past training sessions can also be vital to uncovering the most successful method to present a training course (Hansche 2001).

The NIST 800-50 presents several techniques for delivery format of the training material. Some of them are:

- Interactive video training
- Web-based training

- Non-web, computer-based training
- Onsite, instructor-led training (including peer presentations and mentoring)

For our training, we decided on using the implementation of instructor-led training. As we will explain in a later section, this method proved to be extremely useful in providing training as well as increasing individual accountability.

Evaluation

The training program needs to be evaluated at all phases (Grimes-Farrow 1983). Resources should be allocated for constant evaluation of the training program. Feedback is important at this phase, as changes to the training are made based on feedback from participants and upper management.

There must be a method in place to evaluate the training. Referring again to the NIST SP800-50 document, methods to evaluate the training can include:

- Benchmarking
- Surveys
- Evaluation forms
- Independent observations
- Status reports
- Interviews
- Focus groups (NIST-SP800-50)

After the training package was delivered and completed, we conducted a post-test as well as interviews with select employees and managers to determine the effectiveness of the training. The posttest served as a benchmark that allowed us to measure the effectiveness of the training program. This feedback assisted us in understanding areas that need to be focused on as well as areas where the training process could be improved upon. The results of the testing as well as the interviews that were conducted will be discussed in a later section.

There is no true method to judge the amount of success in a given training program. According to the NIST800-50 standard, there are several indicators that a training program has been a success. They can include:

- Sufficient funding to implement the agree-upon strategy
- Support for broad distribution and posting of security awareness items
- Level of attendance at mandatory security forums/briefings
- Participants demonstrating the skills and knowledge that they have learned

As we conducted this training at several diverse organizations we found that participants began actively demonstrating the principles that they learned. Computers were locked upon leaving, sensitive information was locked away, and both hands were typing for longer than a few seconds at the request of a password. In our view, this was the most rewarding and the greatest measure of success.

Testing and results

Since a checklist is a visual tool which can be used effectively for training and practical purposes, we used one security domain for each area of the checklist we created. This checklist provides the holder with a quick reference or reminder of each security topic for which training was or will be received. We have included a small copy of the checklist below.

This checklist facilitates employee awareness along with accountability. Employee accountability is greatly increased as they sign their initials verifying that they understand each topic presented to them during training. Managers also becomes accountable to the organization when they sign their initials verifying that they have done their due diligence in making sure that each employee understands each domain presented.

A real life example might be helpful in understanding this concept. Jane, who is John's manager, is conducting security training with John. Jane teaches John what the characteristics of a strong password are. She also teaches him how he might create his own strong passwords. She then asks John if he understands this information or to demonstrate his understanding of this information to her. When John signs his initials by this section, he certifies that he understands the contents thereof. When Jane signs her initials, she also certifies that John understands this information. Both Jane and John are working to help John understand how to create strong passwords. Since John knows that once he signs he becomes accountable for the information, he will make sure that Jane explains it clearly. Since Jane knows that once she signs she is accountable for having made sure that John is aware of the information, she will try and make sure that he does in fact understand what was taught. This is a good process for creating individual accountability for information. We have only demonstrated one method but there are other ways for creating individual accountability for security awareness and training.

	Information Assurance Basics	Employee Initials	Manager Initials
1	**Passwords** Should be changed frequently. At least 8 characters, upper and lower case letters, numbers and special characters such as: ! @ # ,) (Example: 17yalwtI = 17 years ago, I went to Italy Example: Mlst7tJ! = My little sister turned 7 this July!		
2	**Social Engineering** Always be aware of who you are communicating with and what information they are requesting from you.		
3	**E-mail** Never send anything confidential over email. Never click on an attachment unless you trust the sender. Communications can be monitored by administrators.		
4	**Physical Security** Properly lockup and secure your workstation upon leaving.		
5	**Locking Computer** If you are not near your computer, lock it or logoff. To lock your computer in Windows XP: windows key + (L)		
6	**Unauthorized programs** Do not install or use any program that is not authorized by company policy.		
7	**Handling confidential data and material** Lockup or destroy any confidential information upon leaving your workstation. Do not let unauthorized individuals view this information.		
8	**Internet** Use caution when visiting sites and strictly adhere to company acceptable use policy.		
9	**Phishing** Delete any emails requesting login or password information via email Or URL redirection.		
10	**Handling storage media and portable computers** Avoid storing confidential information on removable storage devices or portable computers such as CDs, floppy disks, PDAs, laptops, etc. Lock and properly secure removable storage devices at all times.		

■ Checklist

To facilitate the awareness and accountability of these security practices, we created a small version of the checklist to be used as a sheet of reminders for each employee who receives training. The reminder sheet (see appendix) has the same information that the checklist contains with the exception of the two columns used for marking employee and manager initials. The intent of the reminder sheet is that it should be posted somewhere in the workstation where it is always visible for the employee to use as a quick reference. This is simply an optional element to support the awareness gained from the checklist and training.

Most managers or HR trainers are not security professionals and they

themselves may not understand all ten domains presented in the checklist. Since they administer training, it is important that they have reliable resources available for them. Security personnel should be able to train them and the training we created helps provide another reference. If there is a basic understanding already, the training material we created could be used to develop further knowledge and security personnel could be called in as necessary.

An example of the training which we designed based upon the checklist can be found in appendix 2. We included section one and two for view in this article (full version available upon request). The full version includes similar training for all ten domains. This is what we recommend managers use to train employees if their current training material is insufficient. This training is not meant to teach in-depth reasoning for these security measures, but rather, is a very simple and practical training for the non-computer security professional. It is very brief and simple. In conjunction with the checklist, it can be used to help employees gain valuable security knowledge and practices as well as make them accountable for the training knowledge gained.

Commensurate with the domains in the checklist and training, we prepared a quiz that could test current knowledge held by employees in various businesses. The quiz we developed contains ten questions with one question corresponding to each domain in our checklist. The full quiz can be found in appendix 1.

We administered this quiz to 30 different people in various companies within the financial industry. This number is not meant to be a representation of business in general but our purpose was simply to test our assumptions at a minimal level; our sample of 30 is sufficient for this purpose. The businesses include four different banks and two different financial brokerage firms. Employee titles surveyed include managers, bankers, tellers, independent brokers, and secretaries.

Our process began by selecting a business such as a bank or a brokerage firm to approach with our training idea. We asked to speak to the manager and upon meeting with this person we began to explain what we were doing. Most managers became excited for the opportunity and consented to be a part of our survey while others refused. When we received consent, we presented employees with our quiz in order to ascertain the level of knowledge attained in any previous training. We then gathered the tests and instructed the managers on how they could train their employees about each security domain using the training material we provided them. Most of the managers decided to only use our training material to further understand the topics and security principles. One of the managers consented to actually allow one of the primary authors to provide instruction on each domain and the security procedures associated therewith. This was an ideal situation because a security professional could answer any questions that may come up throughout the training process. That manager then presented the training package to the employees in a formal session. The manager's response to the whole process was great.

Before meeting with this manager to go through the training material, we asked what would be an example of a strong password. This person gave us an astonishing answer. Keep in mind that this person works for a bank which is entrusted to protect very sensitive information.

> "I think that a strong password would be something that someone may not think is associated with you. For example, I use the password 'Idaho' because it doesn't have any direct relationship with me personally. If I used something like my last name or birthday, that would be easy to guess."

After going through the training material, this person began to realize the threats that existed and realized how invaluable good security practices could be. This realization by managers is crucial to any training process. Without support from the decision makers of an organization, programs go unfunded and wind up destined to be poor at best.

After the managers were able to train their employees using the training material we provided them, we were able to do a follow-up post-test with some of the same companies. In summary, the process was followed was simple and productive. We conducted a pre-test, provided training through managers, and conducted a post-test. The results of the whole process were encouraging.

Before training, the level of computer security awareness was alarming considering the types of businesses we were surveying. Considering our research and what we had learned from the manager mentioned previously, our pre-test results turned out to be quite predictable. The three most missed questions were the ones about passwords, social engineering, and internet usage. 80% of employees missed the internet usage question, 63.3% missed the password question, and 73.3% missed the social engineering question. We included a table of the quiz results.

Total number of participants	30	Quiz results									
Questions		1	2	3	4	5	6	7	8	9	10
Number missed		19	22	4	8	0	8	2	24	1	4
Percentage missed		63.33%	73.33%	13.33%	26.67%	0.00%	26.67%	6.67%	80.00%	3.33%	13.33%

The answer we were hoping employees would choose for the internet question was that usage depends on the company policy (answer choice B). Upon further analysis, we decided that this question could be deceptive in the fact that if the employees knew their company policy and one of the other choices matched it, that answer choice could be considered as correct. We therefore feel that the results of question 8 do not accurately reflect the knowledge of the employees who took the test. That said, this question is the only one that we have found that could be skewed incorrectly.

The password question is built precisely to ask for characteristics of a strong password. Answer choice C is the only one that contains all four characteristics we listed in the training program. Although the literature we have read differs on what the minimum length of a password should be, we chose to teach a minimum of eight characters due to increasing technological advances and simply to err on the side of caution.

The social engineering question (#2) turned out to be very interesting. The two most popular choices for answers were choices A and C. We were very surprised that nearly half of the people who missed the question chose answer choice A.

Over 25% of all employees missed questions 1,2,4,6 and 8 which in our opinion simply fortifies that these topics need to be addressed more in depth with the employees. In a business that utilizes technology to conduct everyday business and secure information, the ideal employee would understand each topic and be responsible for using good security practices. Companies without good security policies should do all they can to create a policy that will allow them to perform due diligence in protecting sensitive information.

With these preliminary results in hand, we wondered how the same employees would perform on the same test after the simple training session. With consent from a few of the same businesses, we conducted a post-test with their employees. The results improved a great deal since the pre-test and initial pre-training time. For example, the question on passwords (#1) showed an incredible difference. In fact, not one person who completed the post-test missed the question on passwords. The question on social engineering (#2) dropped down from a 73% miss rate to a 33% miss rate.

It is amazing that with an inexpensive and simple training, there was a visible difference among some companies. We were able to interview the same manager we mentioned previously after the employees went through the training program. The comments we heard were very positive.

> "I could actually see a difference in the way my employees thought about security. People were locking their computers when they stepped away, both hands were clicking keyboards for more than half a second when asked for a password, and the overall awareness just seemed to be at a higher level."

In today's business world, employees can be the weakest link or the strongest defense when it comes to assuring information. Simple training with the right tools can increase awareness and personal accountability levels for every employee. Managers need to keep in mind that basic security awareness levels differ greatly between security professionals and non-security professionals, technology can only protect information to the level the users permit, and training can be simple and still be effective.

Conclusion

Information security awareness and training issues are some of the biggest concerns for businesses and the problem will more than likely get worse before it gets any better. The most valuable asset that any business has is people. Security awareness and training is truly one of the greatest protections that a business can have. Increased awareness and individual accountability can greatly affect how security practices are implemented in an organization.

Many firms focus a great deal of resources on firewalls, software, and other types of countermeasures. A security administrator would cringe at the thought of placing an unprotected server on the network that isn't behind the firewall. When people are not adequately trained, we are committing an even worse fallacy. People are by far the most valuable asset and typically receive the least amount of protection. 'Security is only as good as its weakest link, and people are the weakest link in the chain (Schneier 2000). The effects of firewalls and other countermeasures are greatly diminished if we do not adequately protect our most valuable asset.

As has been shown by this exploratory study, impressive results can be seen from a simple training program that virtually any organization can easily implement. The exploratory study showed a great deal of personal learning occurred as individuals were personally instructed in each of the ten domains. Based upon the five phases of a successful program, we measured our success as two fold. First, the post-test showed increased awareness and understanding when compared to the results of the first quiz. Second, after the training, several employees could be seen locking their computers, typing stronger passwords, and storing confidential information securely. We believe this to be the true measure of success.

We also believe the success of the exploratory study is strongly correlated with the raised awareness and small portion of accountability established by managers in the training process. If this training method was fully implemented in an organization, individual accountability could be greatly enhanced making the possibilities of success truly limitless.

We firmly believe that it is vital to increase awareness and individual accountability using the proper tools for any training program to be a true success.

References

[1] Schneier B, John Wiley and Sons (2000), *Secrets and Lies, New York, NY, USA*

[2] Coverstone, Paul D. (2003), "IT training assessment and Evaluation: A Case Study," *Association of Computing Machinery*

[3] "The 2005 CSI/FBI Computer Crime and Security Survey" (2005) *Computer Security Journal* Vol. 21, no. 3

[4] NW3C & FBI, 2005 'IC3 2004 Internet Fraud – Crime Report' http://www.ifccfbi.gov/strategy/2004_IC3Report.pdf

[5] ISO 17799, BS ISO/IEC 17799: 2005

[6] Dagada, Rabelani (2004), "'Where have all the Trainers Gone?' E-learning strategies and tools in the corporate training environment," *South African Institute for Computer Scientists and Information Technologists*

[7] Hansche, Susan (2001), "Information Systems Security, Training: making it happen," *Security Management Practices*

[8] Moore, Sue (2003), "Training Program Growth…From Flat Line to Pulsating," *ACM Press*

[9] Peltier, Thomas R. (May/June 2005), "Implementing an Information Security Awareness Program," *Security Management Practices*

[10] Pfeffer, Joleen (2003), "Deep in Benchmarking: Using Industry standards to Assess a Training Program," *ACM*

[11] Bradford, George (2003), "What's Old is New Again: Training is the Information Technology Constant," *ACM Press*

[12] Grimes-Farrow, Dorothea (1983). 'Human factors training and awareness'. ACM conference on Computers : Extending the human. Jan 5-7. New York, NY. [13] Schell, Bernadette H. and Martin, Clemens (2004), Cybercrime: a reference handbook, Santa Barbara, California.

[14] Desman, Mark B. (2003), "The Ten Commandments of Information Security Awareness Training," Security Management Practices, 11(6): 39-44.

Appendix 1

Information Assurance Basics Questionnaire

1. Which of the following has the most characteristics of a strong password?
   a) asdf8w4ajl
   b) pneumonoultramicroscopicsilicovolcanokoniosis
   c) J74almh!
   d) DoeJohn2

2. Which of the following is an example of social engineering?
   a) Jane only invites company employees to the company party.
   b) Someone calls a bank teller and wants to know Jim's account number so they can make a deposit to his account.
   c) Someone is able to guess the password Jane uses for internet banking to access her financial information.
   d) Tom only buys Pepsi out of the company vending machine in order to maintain his social reputation.

3. Which of the following should you never send via e-mail?
   a) attachments
   b) company stock price
   c) personal customer information
   d) all of the above

4. Which of the following is an example of physical security
   a) Locking the door to your office
   b) Logging of your computer
   c) Turning off your computer when you go home after your shift
   d) None of the above

5. Which of the following is good security when you leave your computer?
   a) Turn off the monitor
   b) Unplug your keyboard and mouse
   c) Ask someone to make sure nobody uses your computer while you are gone
   d) Lock computer

6. Which of the following might be an example of an unauthorized program?
   a) Internet Radio
   b) An instant messaging program
   c) A game you downloaded from the internet that may contain viruses
   d) All of the above

7. Which of the following may contain or display sensitive data and/or material?
   a) A copy of a customer's records
   b) A floppy disk
   c) Your computer monitor
   d) All of the above

8. How should you use the internet at work?
   a) Only view pages that don't contain harmful applications
   b) It depends on company policy
   c) Never use the internet for other than work purposes

d) Only use the intranet, not the internet

9. What kind of information might you be asked for in a phishing scam?

a) Your street address
b) Your user ID and password
c) Your social security number
d) All of the above

10. Which is an example of storage media and/or a portable device?

a) A floppy disk
b) A computer hard drive
c) A laptop
d) All of the above

Appendix 2

Information Assurance Basics Training

I. Passwords

A. Dangers
   1. "80% of all network security problems are caused by bad passwords."[1]
   2. Bad passwords can allow intruders access to your financial information and the possible theft of your identity.

B. Passwords should contain
   1) At least 8 characters
   2) Upper and lower case letters
   3) Numbers
   4) Special characters such as: ! @ # ,) (

C. Methods to remember extremely strong passwords
   1. Turn a full sentence into a password
      a. Example: **17 y**ears **a**go, **I w**ent **t**o **I**taly.
         i. 17ya,IwtI
      b. Example: **M**y **l**ittle **s**ister **t**urned **7 t**his **J**uly**!**
         i. Mlst7tJ!
      c. A password should be guarded with the utmost care and never divulged to anybody.

Teaching tip: Two most important areas to focus on are the importance of frequent password changes and selecting a strong password.

Discussion point: *A simple passwords such as "Idaho" can be broken in less than two minutes. On the other hand, a more complex password such as "Mlst7tJ!" would take almost two thousand years to break.*[2]

II. Social Engineering

A. Dangers
   1. "Amateurs hack systems, professionals hack people"[3]
   2. A password or any other confidential information is only as confidential as people are willing to keep it.
   3. Social engineers often prey on sympathy or desire to avoid conflict.

B. How to combat Social Engineering
   1. Social engineering is an attempt to manipulate legitimate users to gain unauthorized information.
   2. Always be aware of who you are communicating with and what information they are requesting from you.
   3. Don't give out information (no matter how insignificant it seems) to someone who isn't authorized to know it.
   4. Don't offer supplemental information that is not necessary.

e.g. If Linda is gone for the day and someone calls up and asks if she is in, don't tell them that she always takes the third Friday off. Just tell them she is not in. Be aware and be careful.

[1] http://www.foxnews.com/story/0,2933,172014,00.html
[2] http://geodsoft.com/howto/password/cracking_passwords.htm#howlong

[3] Bruce Schneider