(Note: Set up room using Accelerated learning peripheals, i.e. Star wars Posters, objects on tables, colored markers in colored cups, pens at each seat, name cards at each seat, Learning Mural on wall, write objectives on flip chart to display during session)

Introduction *(10 minutes)*

Objective: Confirm objectives; set tone for training; orient participants to class and facility.

- Welcome the group.

Introduce yourself.

Explain course objectives. (refer to flip chart)

Conduct icebreaker. – Have participants pair off in two's. Inform the pairs that they will introduce each other to the group. They will need to collect the following about their partner:

Name

How long at Texaco and which areas have they worked in

In the relm of security, which issue is most important in the scope of the work you are involved in at (company name). *Protection, Detection or Reaction*

- Cyberwar video **(15 minutes)**

- Case for Action video by program executive or other leadership sponsor (to provide the Why we are doing this information) **(5 minutes)**

- Short break **(5 minutes)**

Support Materials

Welcome

Objectives

Introduce activity – How Can You Apply This to Your Job: Explain that periodically during a course, you will provide an opportunity for participants to list on an idea card, 3 ways they can apply a particular security protection, detection or reaction skill to their job. Quick - allow 2 minutes for this activity. The ideas will be collected and posted to Learning Mural. After the workshop, ideas will be collected and used in additional applications (newsletter, intranet postings, etc.)

Personal Security ***(15 minutes)***

Objective: *Cover areas of Personal Security (social engineering) definition, areas of vulnerabilities. Cover how to protect against, how to increase awareness so you are able to detect and how to react if it occurs.*

Show PowerPoint Presentation .

Introduce the topic objectives via PowerPoint presentation.

Explain more information. Share some personal examples.

Write your personal example here:

A group of outside auditors entered the building at a clients place of business the same time I did during one of my early morning visits. The guard asked that they all sign in.

One of the auditors went to extremes to "smooze" the guard, and after building a relationship asked "You don't mind if I sign in for everyone, do you?"

Without missing a beat and continuing to smile, the guard explained that although it would be more efficient, it would be necessary for each auditor to sign in for themselves. She offered to provide more than one sign in sheet to hasten the process.

Key points: if you need to approach someone, remember to remain calm and polite. Example: a simple "May I help you?" can appear helpful, yet confronts a potential threat to securtity.

Examples of Personal security issues include:

- **Calling users and acting like computer support staff.**
- **Obtaining access to the physical building (temp staff, janitorial staff).**
- **Dumpster diving.**
- **Acting as a phone company employee.**
- **Wearing a suit and using fake business cards or another individuals business card.**
- **Shoulder surfing.**
- **Payoffs to security personnel, hotel staff.**

Personal Security (Cont.) ***(15 minutes)***

- Conduct an activity.

- Debrief the activity by asking questions such as:

  - *Question 1. Can anyone provide some of the responses that you practiced?*

  - *Question 2. Anyone identify any that are somewhat uncomfortable?*

  - *Question 3.Can anyone provide any tips to make these situations more successful?*

- Summarize this section by….

"To review, a person that will deceive or 'con' others into divulging information that they wouldn't normally share is a threat. These threats can happen in person, over the network or through the phone. Knowing how to detect a situation and how to react if a situation occurs is key!"

Instruct participants to pair off in two's. Provide each pair a set of Modified Role play cards.

Role play 1 – confronting someone without a badge

Role play 2 – Approaching and responding to a stranger in the building that is alone

Role play 3 – Phone call

Role play 4 – Network

Break **(5 minutes)**

Physical Security ***(15 minutes)***

Objective: Summarize objectives for this section.

Introduce the topic .
Transition:
• When discussing controls, identify how they help protect the employee.
• When requiring employees to wear identification badges, many security programs tell the employees that this has been implemented to meet
security objectives.
• What does this really mean?
• What the employees should be told is that the badges ensure that only authorized persons have access to the work place.
• By doing this, the company is attempting to protect the employees.
• Find out how controls support or protect the assets (including the employees) will make the security program message more acceptable.
. "*Just because you are in an office building does not mean everything is as safe as it is in a fairy tale.*

Outside influences can disrupt our normal work day.

The key is knowing how to prevent a situation from happening"

- *Explain more information. Share some personal examples.*

Write your personal example here:

A soft-drink deliveryman opened the door into a secured area by using the keypad. Startled, I turned to the manager I was interviewing and asked if he had seen this flagrant breach of security. "Oh yeah, no problem," he replied. "We got tired of opening the door for him every week, so we gave him the combination to a secured area."

Mention the conflict between how this situation can be perceived differently by different people.

One employee just sees a deliveryman that they have known for a long time and trusts completely. Someone else that has a knowledge of information protection might perceive this as a delivery man that has some friends that could be a big security risk.

Let's look at personal security vulnerabilities, and how to Protect, Detect and React in situations.

PowerPoint Presentation on Physical Security

Physical Security (Cont.) ***(25 minutes)***

- Conduct an activity. Video, pictures and other mediums depicting Physical security situation will be shown to participants. Participants will be asked to provide examples of Protection/Detection/Reaction behaviors for each example. A Knowledge Globe (soft globe) is used to toss from participant to participant as a means of selecting someone to provide an answer. Participants can also ask to have the Knowledge Globe tossed to them to provide a response.

- Debrief the activity by asking questions such as:

  - *Question 1. Are there any other responses to any of the situations that someone can add?*

  - *Question 2. The issue of Protection/Detection/Reaction is important because knowledge without action is not much better than no knowledge at all. Can anyone provide an example of a situation when they did all 3 and how it turned out?*

  - *Question 3.Can anyone provide a successful response to a "tailgater"?*

- Summarize this section by….

"If you ever lose your access card or key, make sure to report it immediately so it can be deactivated and you can get a new card.

Maintain a 'clean desk' by putting files and other information sources away when not using them.

and finally, when you leave late at night, try to exit with other co-workers."

- Short break **(5 minutes)**

Alternate activity - Stump the Class: Assign teams of 3-4 people per team and give each team 3 index cards. They are to write a review question and answer on each card that would test the class's knowledge of the topics covered so far. They have 10 minutes to review all their training materials and come up with the questions. The trainer collects the cards and tosses a ball randomly to ask a question. The person who catches the ball may answer the question, confer with the team, or toss to ball to someone else. Once the question has been answered correctly, the person who has the ball tosses it to someone else and the process continues until all the questions have been answered.

Information Security ***(15 minutes)***

Introduce the topic .
"It is important that we protect our organization's information.

Why? Let's take a look at some reasons...
maintain customer confidence (prompt discussion of what this means and how this could be affected by a loss of information)

- maintain public image (prompt discussion of what this means and how this could be affected by a loss of information)

- remain competitive (prompt discussion of how we could lose in competitive situations if the wrong information were made public)

- protect ourselves and other employees (prompt discussion on how much personal information the organization has in it's systems and also how well each of us knows some of our co-workers and their families)"

"What is the importance of keeping our data confidential?

Information has value
- monetary value
- proprietary value
- competitive value
- personal value
The previous sections talked about how we can prevent others from getting into information at our work station.
The next few sections will discuss how we can avoid accidentally providing information to the wrong entities."

- Explain more information. Share some personal examples

- PowerPoint Presentation on Information Security

Information Security Activity

Activity for Information Security **(25 minutes)**

Start with:

Match the password with its critique.

	fido	**1** Moderately strong but possibly flawed - uses letters and numbers, is longer than 6 characters, but is a easily guessed if the user is a Washington Redskins football fanatic - passwords should not relate to one's family, cars, pets, or hobbies.
	tbzntb	**2** Strong - has more than six characters, uses numbers and letters, is not a recognizable word, and can be remembered by thinking of President Lincoln's question, "How many legs would a sheep have if you called a tail a leg?" (Of course, the answer Lincoln was looking for, wasn't 5, it was 4, because calling a tail a leg doesn't make it a leg.)
	riggins44	**3** Moderately strong - has 6 characters, not a recognizable word, but doesn't use numbers or special characters, hard to memorize.
	sheep5leg	**4** Weak - too short, is likely the user's pet's name.

Follow up

Galatic Learning Summit – have teams play the role of two nations sharing knowledge at a “learning summit”. Each team receives material to research and then bargains for information held by the opposite team.

Group 1 is assigned the title Password Construction experts and provided the following information:

1. The more complex and random it is the harder it will be for someone else to crack. Of course it may also be hard for you to remember, so you should try to choose a complicated password which is also relatively easy for you to remember, but hard for someone else to guess.

2. Use at least 7 characters in the password. Shorter passwords are easier for computer programs to guess. Newer versions of Unix require that you use at least 6 characters in a password, and that at least one of them not be a letter. But remember that most Unix passwords are only 8 characters long - any extra characters are simply ignored.

3. Just adding a number or punctuation mark to a word can make a password a bit more secure, but if it's a dictionary word then this will probably not enough. One well known cracking program easily caught the password "offbeat1". A better combination would be "off1beat".

4. Use fragments of words mixed in unusual ways that would not be found in a dictionary, or take a compound word and swap the pieces in an unusual way. The password just suggested above is even better if you swap the first and last parts.

5. Obscene words are generally not good passwords, even though they may not not be in on-line dictionaries, because many cracking programs check for these separately.

6. Take a word and substitute a symbol or number for one or more letters. But be unusual. Many cracking programs already know enough to try a "$" in place of an "S", or a "1" in place of an "I" or "L". It's better to just insert punctuation, numbers, or special characters at random in the middle of a word.

7. One way to make a good password is to take the first letters of a phrase you can remember. Use a poem you like, a song lyric, or a quotation you can remember - the more obscure the better. A phrase that only means something to you is even better. This produces a sequence of letters which you can remember, but which nobody else can easily construct, nor remember if they see it. The password will be even better if you insert or substitute punctuation and numbers, as in the previous rule.

8. Another way to make a good password is to interleave two words, or a word and a number. For example, mixing "July" and "1776" gives "J1u7l7y6". (But that's a bad example, because it's a well known date - use something more obscure.)

9. **OLD** car license numbers (or aircraft "N" numbers) make good passwords, but the license number of the car you are driving now could be easy for someone else to guess. "NCC-1701" is not a good password - too many crackers watch Star Trek.

10. Words from other languages are better than English dictionary words, but can still be cracked if the cracker has an on-line dictionary in that language (many are easily available). Applying some of the tricks mentioned above to foreign words can lead to a good password, as long as you can still remember it.

11. Another way to generate a password which someone else can't guess is to use input from a physical object in your possesion. For example, the serial number on the bottom of my answering machine is "93-195M", and that is a good password which cannot be guessed by a dictionary program. But be careful with this method. If someone in my office knows I pick passwords this way, then one of the first things they will do is look at the bottom of my answering machine.

12. Along the same lines, the serial number of a dollar bill, or some subsequence derived from it, can be used as either a password or as a good reminder of a password. Keep the bill in a safe place - don't spend it. You can even share the password with someone else by tearing the bill in half.

Good Security Practices **Create a strong password**

- **Use at least seven characters, eight is better.**
- **Use characters from at least three of the following four classes:**
  - **English upper case letters**
  - **English lower case letters**
  - **Westerrnized Arabic numerals (0,1,2,...)**
  - **Non-alphanumeric (special) characters such as punctuation symbols.**

- **Don't use any part of the account identifier (logon ID, Operator ID, etc.).**
- **Don't use a proper name or any word in the dictionary without altering it in some way.**
- **Don't use obvious phrases or sequences such as "GOBUFFS" or "12345".**
- **Don't reuse a password you have used before: construct a new password each time you change it.**

Group 2 is assigned the title password management Experts and provided:

Here are some guidelines to help make your passwords more secure:

1. Change your password often. Even if someone cracks the system password file, the password they obtain is not likely to last long. It can be hard to remember to do this, so use something else to remind yourself. If you change your password once a month, do it at the beginning of the month when you pay your bills, or change it every quarter, at the timewhen you pay your bills. Change it at least once every 3 months. Some computers have "password aging" which forces you to change your password often. This is good as long as it's not often enough to be annoying.

2. Never give your password to anybody. The computer center staff don't need to know it, and in fact they can't find out what your password is (without running a cracking program themselves!). If you get e-mail from someone asking for your password so that they can trap a cracker, then they are probably a cracker themselves. Report it to the computer center.

3. If you think someone might have seen you type in your password ("shoulder surfing"), then change it as soon as possible. On any Unix computer the command to change your password is `passwd` (though you should check for local variations).

4. If you can avoid it, don't write your password down. If you do have to write it down, don't label it. If someone sees "xyzzy" in your notebook they may not know what it means, but if they see "my password is xyzzy" they will. [And by the way, "xyzzy" is a magic word from a computer game, so it's not a good password.]

5. If you work on more than one computer and they don't share a common password file, use different passwords on different machines. Then if someone breaks into one computer they still can't get into the other.

6. Use private information known only to you when you construct your passwords, not public information which other people are able to find (no matter how unlikely you may think it would be that they would find it - if it is publicly available don't use it).

7. Never send a password through e-mail! Electronic mail is not as secure as you might think. If you have to send someone a password, use regular mail or fax, or encrypt your e-mail., if possible.

Maintain the security of your password

- **Don't write down your password: remember it. It's better to have your password reset because you forgot it than to have it stolen.**
- **Don't use a weak password just because it's easier to remember. If you can't remember your passwords, write them down in a secure place where you'll know right away if they've been stolen.**
- **Don't give your logon or password to ANYONE! Don't give it to your supervisor, your spouse, your friend, the school president, your mother, or any other authority!**
- **You are responsible for ANY activity done with your accounts.**
- **Don't let anyone observe you entering your password. Cover your keyboard when logging in if someone is watching you, or ask them to turn away.**
- **Change your password at least every 60 (variable) days.**
- **If your password has been changed or reset and you didn't request it or change it, please let us know!**

Other good security practices:

- **Don't leave your workstation logged on, and unattended for long periods. Protect yourself by installing an approved software locking screen saver with a short activation interval. Logout during lunch and before leaving for the day.**
- **Avoid downloading and installing unknown or unapproved software on your PC, workstation or Unix nodes. You could be downloading viruses, trojan horses or worse.**
- **Avoid bringing files or software on floppy disks from public PC's or workstations to your business workstation.**
- **Scan disks or downloaded files for viruses before doing any other type of access, even something as innocent as a directory command. This will prevent the spread of viruses.**
- **Lock your office if you can. Physically secure your PC to your desk if it is located in an easily accessible place. Consider installing a special card that will sound an alarm if the workstation is moved and/or spray dye on the internal parts if the cover is removed by an unauthorized individual. Parts like memory and CPU chips make a great target.**
- **Put password protection on files you store on your workstation or LAN server when they contain sensitive data or data downloaded from a company database.**
- **Don't throw away sensitive paper copies of data, customer information, userlists, programs, network diagrams, etc. Dispose of these properly, shred or eat them!**
- **Don't distribute files on floppy disks that have had sensitive information previously written to them. Use a new disk. Prevously written information can be read from this media.**

Conclusion

As Clint Eastwood once said,
"If you want a guarantee, buy a toaster." The only secure system is one that's unplugged, turned off, and in a locked room.

Since it's not practical to leave our systems turned off, we need to understand the risks to our systems and prepare ourselves to defend them. Preparation begins with understanding - and that's where awareness comes in.

With all the news stories about hackers, viruses, and network break-ins, it's easy for the security message to sound over-used and tired, like Peter, the Boy Who Cried Wolf. It's too easy for people to say, "Yes, but it won't happen to me" or "It won't happen here."
Security apathy and ignorance are the biggest threat to our computer systems. . . . And the best way to achieve a significant and lasting improvement in computer security is not by throwing more technical solutions at the problem -- it's by **raising awareness** and training and educating all computer users in the basics of computer security.
Say "Just as steps have been to taken to ensure the safety of the employees in the workplace, the organization is now asking that the employees work to protect the second most important enterprise asset - information. If the organization fails to protect its information from unauthorized access, modification, disclosure and/or destruction, then the organization faces the prospect of loss of customer confidence, competitive advantage and possibly jobs. All employees must accept the need and responsibility to protect our property and assets."

Evaluation

Ending Activity –

Give each person a post card. Have them write their name and address (or e-mail address) on one side and a goal they plan to achieve in the next month on the other side. Collect the cards and send them out to participants 1 month later, asking them for feedback about how well their goals have been met.