Security Awareness
Incident Response Scenarios
Experiential Learning for Meetings or to Supplement Presentations

General instructions: Partners choose 2 role-play situations to work on. Each participant takes one to respond to while the other takes notes. (2 ½ minutes each) After the role-play participant has finished, the note taker adds additional ideas. Once both participants have responded to their situation, gather the notes and be prepared to report back to the group.

All: Collect any **Protect, Detect, React** ideas that surface and add them to the learning mural.

Role-play 1 - Ask a colleague not to step through a secured entrance without passing through the access-control system with their own identity. Assume that they are not happy with your response, since they have always "slipped" through and they are late for a meeting.

Role-play 2 - Tell your co-worker that you will not copy Vendor software without a license to do so.

Role play 3 - You have just encountered a visitor or another employee walking towards you and notice that they are not wearing an identity badge. What would you say to them? What would you do?

Role Play 4 - You have just received a phone call from someone that identifies themselves as a vendor for your manager. They ask for some information that you're not sure should be shared (i.e., confidential company information). What would you say to them? What would you do?

Role Play 5 - Someone visiting your office area is unknown to you. They ask for some information that you're not sure should be shared (i.e., confidential client information). What would you say to them? What would you do?

Role Play 6 - You have arrived at work early one morning and are greeted with the following email.

Hi,

My name is Ted Dehanson and I am the system administrator here at domain.com. We recently had a security break and are re-assigning passwords to users. We would highly recommend that you change your password as soon as possible to the randomly chosen password below.

Your randomly chosen password is: **abc123**

Thank you,

Ted Dehanson

What can you do?

Role Play 7 While working on the employee payroll database, Georgia was called away from her desk to attend an urgent meeting. Upon her return, she noticed that some of her paper files had been moved and that her computer was still logged on to the payroll database, but it was in a different module than when she left for the meeting.

1. What steps could Georgia have taken to prevent unauthorized access to confidential employee files?

2. Which desktop security measure would have almost completely alleviated the risk of disclosure of confidential employee information?

3. What could Georgia do if adequate space/security isn't readily available (i.e., order locking file cabinets, ask for a desk/door lock, etc.)? ?

4. What are the risks associated with the unauthorized disclosure of confidential company information?

Role Play 8 - John, Sara and Alex are all new employees who have been assigned user accounts. Initial passwords have been assigned to all three users, who have been instructed that when they first log on they must select a new password 9they are to follow 's password selection standards and guidelines).

John chose john1999 for his password

Sara chose cvbnm as her password.

Alex chose zH9mT1 as his pasword.

1. Which is the strongest password and shy?
2. 2. Why are the two passwords you did not select weaker passwords?
3. 3. Suppose a new employee selects Gomen! (The Japanese word for "excuse me' or "I'm sorry") as her password. Would this be considered a strong password? Why or why not?
4. (Note that Gomen! is not in the English dictionary, it has a non-alpha character included, and the first letter is capitalized – all of which can be attributes of a strong password).

Role Play 9 - An employee learns that another employee has used their logon id & password and has been sending inappropriate emails or subscribing to non-business related Internet sites or sending confidential information to another company. Discuss ways this situation should be handled.

Role Play 10 - You come back from lunch and you notice the security door is propped open with a chair and there's a note stating "Pizza Person: Bring the pizzas to room 3418". What should you do?

Role Play 11 - The IBM person is at your desk asking you to tell him your password so he can do some work on your system. You have always given him your password in the past, what should you do now?

Role Play 12 - You notice a distinguished man in a three-piece suit with a nice leather briefcase in your head quarters building. He's not wearing a badge, but you're positive he must be an executive, as no one but executives wear suits is this building. What should you do?

Role Play 13 - Just as you're getting your desk cleaned up at the end of the day, a co-worker comes to you and says, "I've shut down my terminal, and I need to get produce a couple of reports. Since you're leaving, let me get on your terminal and I can get out of here too." How would you respond?

Role Play 14 - While at a social function, a friend introduces you to another person. You proceed to have a conversation with the person after your friend describes you as "that IS expert I told you about." Having been described in that manner makes you wonder a little, but the new person proceeds to tell you that they've heard amazing things about your organization. The conversation continues, with you describing in general terms the decision-making support capabilities of the IT system. Then the person asks you some technical questions involving the systems configuration and remote access, as well as some very detailed questions about specific reports. What would you do, both immediately and as a follow-up action?

Additional Role Play