Training is often advanced as the solution to information security problems. This leads one to ask "what should be taught," "how should it be taught," "the role of punishment and reward," "who should do the training," and "how can we find out how effective the training has been?"

Discuss the role of training in helping ensure compliance of security procedures. Your essay should answer the questions raised above and also suggest areas of security where training will be more effective than others.

You should then consider an organisation dealing with patient information in the National Health Service, and outline a training program for doctors, nurses, secretaries, managers and security staff.

Your essay should reference the papers on the course collection to back up your statements and recommendations.

What follows is an example of the points that could be made. I am looking for a well structured and reasoned argument that references the papers as support. Students should be aware of viewpoint of the paper's authors and that they may well have their own agenda. If there are competing arguments in the literature then both side of the argument should be summarised.

What should be taught should focus mainly on how the individual's behaviour affects security, although an overview of the larger security situation should be provided. Individuals should also be taught about general social engineering attacks. What is taught will depend on the individual's role. Obviously individual's accessing sensitive data need training, but decision makers also need to be trained in threats and the effectiveness of various security solutions.

How should it be taught should reference the studies showing that in general security training is not very effective. Role playing and simulated attacks are more effective. Also, training needs to be reinforced regularly.

Punishment and reward should fit the importance of security to the job role. The goal should be to make the individual more effective, from a security point of view, after reward or punishment.

The choice of who to do the training depends on the size of the organisation. In many cases, specialist training contractors are a good choice. Their core business is training and so they can become good at it. They are also outsiders and less of a threat to the people they are training. An internal training department may be a good idea because they have company specific information. In practice, however, training tends to become the dumping ground for ineffective personnel. Members of the IT security staff tend to make poor trainers unless they are dealing with deep technical details.

Evaluating the effectiveness of the training is difficult because the aim of good training is for nothing to happen, no security breaches. Also, detecting successful defences against attack is rather haphazard. Simulated attacks seem the best way of evaluating the effectiveness of training.

In the NHS example, I am looking for training against social engineering attacks and sloppy data management. For example, doctors can be trained not to bypass security to get at information quickly, secretaries should not forward medical details to a doctor at another hospital as a favour. Managers should be careful about releasing aggregate data to researchers and understand how to anonymise data.