CSI4139
Lab 5
NamChi Nguyen - 7236760

Group members:
Julian Templeton - 8229400
Sean McAvoy - 8263210

(a) Discuss what these objectives are and the kinds of constraints that need to be considered.
In CyberCIEGE, we play as a security officer that must make decisions that'll ensure the security of the organization from attackers. Some objectives of a security officer include maintaining the network, the hiring and training of IT staff, physical security, network/software/application configuration, creating and following security policies, the purchase and installation of software like antivirus, intrusion detection, etc. from third party vendors which all contribute to protecting a company and its assets. Some kinds of constraints that need to be considered are the budget, time and available resources to follow and implement the security practices.

(b) Do you feel that CyberCIEGE does an adequate job of illustrating the difficulties and uncertainties involved in the security officer's job? Why or why not?
Yes, I think CyberCIEGE gives a good introduction to the basics in understanding and handling the difficulties and uncertainties involved in a security officer's job. Although we didn't play through all the scenarios, there are a wide variety that would let us familiarize with access control with integrity and confidentiality security policies, firewalls and VPNs, PKI, and many others. Some types of attacks that we'd have to face would be against internal threats, viruses, Trojan horse, DoS, and trap doors [1]. It allowed us to see the repercussions of our poor choices and outlined the possibilities that could arise should a security officer make unwise decisions.

However, it doesn't portray any business aspect of the company and how a security officer may have to be aware of the business objectives of the company when it comes to formulating a decision that may increase the security but have an impact on the company's goals.

(c) How could the game be modified to more realistically portray some of the security officer's day-to-day activities and concerns?
The scenarios we've played in-game only show the impact of the security officer's decisions within one day, particularly in a span of a few hours. Although, realistically the attacks and threats that occur can take place over weeks, months or years depending on the scale and severity of the attack. The game doesn't seem to allow a scenario to simulate more than a day and it could be modified to have the simulation run a scenario ranging from a week to a month or more.

(d) Name one thing that you learned from each game scenario that you completed.
Training scenarios:

- *Stop Worms and Viruses*: to complete this scenario, one had to ensure that users were cautious of email attachments. I learnt that this also included .doc files, but it is a necessary risk as Word documents are used on a daily basis in the workplace. To mitigate the risk, antivirus software should be up-to-date, and employees should also receive training.

- *Life with Macros*: to complete this scenario, one had to ensure that the antivirus software was automatically updated. Since macros can be executed in word documents and spreadsheets, I learnt that an up-to-date antivirus software is the best way to mitigate the risk. However, if the document received is from a trusted source, it is safe to run the macro, but to be extra cautious, every macro should be disabled by default and only executed after it's confirmed benign.

- *Identity Theft*: to complete this scenario, one had to protect a user's personal computer from identity theft by making sure antivirus software was up-to-date and that the user was cautious of email attachments. I learnt that it is important for a user to take every necessary precaution when browsing online and to not accidentally give or reveal sensitive when accessing unsecured websites.

- *Passwords*: to complete this scenario, one had to reinforce good password management and good password policies. I learnt that it is important for users to be educated on creating strong passwords although the criteria to create one such as the password length and character set should generally be of medium length and a moderate set respectively. This is because if the password length is too long and complex, the user in the game was unable to remember their password.

Starting Scenarios:

- *Introduction*: this scenario required us to buy computers for 2 users and set up a basic network. One of the users was able to maliciously alter source code despite a good password policy. One had to ensure that computers were automatically locked if left unattended. I learnt that even though a user has a strong password set up, if they don't lock their workstation, even to leave for a minute is a bad security practice. Employees should be educated to always lock or log off from their computer regardless of how much time they plan to spend away from their workstation because a secure password can only help if the computer is locked in the first place.

- *Physical Security*: this scenario required us to buy equipment to maximize the protection of data of different clearance levels such as Secret and Top Secret. I learnt that depending on the confidentiality of the data, one would have to consider how the data must be physically protected, whether it required hiring guards to patrol around a restricted area or the consideration of biometrics and types of locks used.

References:

[1] Naval Postgraduate School, “CyberCIEGE”, n.d., [Online]. Available: https://my.nps.edu/web/c3o/cyberciege. [Accessed: Nov. 28, 2018]