**CPSC 525 – Assignment 1**

**Alex Stevenson – 30073617**

1. **Assets, Vulnerabilities, Threats, & Controls**
2. **Choose a specific social network  
   Social Network**: Facebook  
   Facebook is the most user-centric social network. Users set up a profile of personally identifying information and can add various types of posts to their user wall for anybody to view or interact with via reactions and comments. Users create a network of friends to interact with, where friends automatically get updates on each other's profiles and can message each other directly through the secondary *Facebook Messenger* app.  
     
   Facebook offers various additional functionalities such as User Groups and Public Business Profiles. User Groups are created by group administrators that link member profiles together where member profiles can post and interact with the group, receiving notifications whenever the group is updated. Public Business Profiles are special accounts created for businesses that include extra information such as a business phone number and special events that the business can create. Business posts can be advertised to users based on user interaction history.  
     
   Facebook also contains a marketplace for individual users to add listings and perform transactions between people. These transactions and interactions with listings are tracked by Facebook to better personalize advertisements towards users based on their financial activity.
3. **What are the most notable assets?**The primary asset of Facebook is the immense amounts of information that it collects on everything and everybody. This has resulted in numerous lawsuits and scandals but Facebook continues to collect exceptional amounts of data, primarily for selling to advertising firms and other companies for financial gain.  
    **User Assets**: Personal user information, authentication information, geographic location, finances and marketplace habits, posting ability (malicious actors posting detrimental information), messenger chat history, interaction history with other posts and the marketplace  
   **Business Assets**: Authentication information, employees, marketplace listings  
   **Group Assets**: Administrator information, user list
4. **How do you think someone might attack the social network or its users?**The main threat is social engineering performed on users to gain access to their information that is linked to their profiles. This can gain their authentication information to access their account, to then access their personal information. Social engineering can also be performed on the marketplace, to simply scam other users through real-life transactions. Once a user's authentication information is stolen one can also post publically on their user account, either posting malicious information about the user to cause social harm or spreading false information through otherwise trusted profiles.
5. **Who are the primary adversaries that might target various threats?**Amateur hackers targeting users can cause social harm to the user as detailed above.  
   Government agencies or hacker groups can target prominent profiles to post propaganda to further a political cause.  
   Marketing firms may target groups, businesses, or Facebook itself to acquire mass amounts of personal user information for advertising or other business related purposes.  
   Other groups may do the same to gain personal information to sell for financial gain.
6. **What are some reasonable controls to help mitigate the threats you identified?**Prevent Facebook from collecting such an insane amount of data on individual users. If they were more limited in their personal data collection then they would be less useful to potential adversaries that are trying to do societal harm.  
   Implement Two-Factor Authentication for Facebook accounts across several devices to minimize the risk of social engineering to easily gain authentication info.
7. **How do you think someone might use the social network to implement attacks or defenses affecting other networked systems?**Gaining personal authentication information on a user could allow you to use that same authentication info to try to access their accounts on different systems.  
   You could use a user's public posts to try to gain insight on security questions across other systems (such as the name of their first pet or their mother's maiden name)  
   With access to enough personal imagery of the user, AI generated deepfakes could be created of that user to destroy their reputation or further political goals.
8. **What are the most important security concerns for your chosen social network?**As Facebook is centered on individual users, the primary security concerns are certainly the individual users and the ridiculous amount of data that Facebook collects on them. Being able to access the data on different users can be used in various ways to harm those individuals and society as a whole. The easiest way to access systems that you shouldn't be able to is through the massive amounts of people that are present on facebook.

**3. Security Review**