Question 1

1. On August 8th 2008, an article warning Facebook users about a worm attack was published on the CBS news website under the CNET Tech News section. In the article, it was reported that Sophos, a security software and research company had discovered a new malware attack that was targeting the comment walls of Facebook users. Users were lured into clicking on a video or image by public wall posts claiming to be from someone on their friends list. Instead of leading to something that was supposedly hosted on Google.com, users were directed to a photo of a grinning court jester with its tongue out and a downloaded Trojan. At the time of this article, Sophos was still investigating the issue and no mention of what the worm actually did was made. In a later update of the article, Facebook released a statement saying that they had been working on a fix for the worm and only about 0.02 percent of Facebook users were affected by this incident. The article also quoted a Sophos analyst, Graham Cluley, warning companies about the security risks that came with allowing their employees to access social network sites such as Facebook and MySpace during work hours. Previous warnings by Sophos and other security firms about the vulnerability of social network sites were also reiterated. The article concluded with some security suggestions from Facebook to its users.

Reference:
[1] Caroline McCarthy (2008, Aug 08). Facebow Users Warned of Worm Attack. CBS News. [Online]. Available: http://www.cbsnews.com/stories/2008/08/08/tech/cnettechnews/main4331903.shtml?source=RSSattr=SciTech_4331903

2. In this incident, the assets at risk could either be of personal or corporate value. Victims of the worm who were using their personal computers could cause damage to their home computers. If the victims had been accessing Facebook during their office hours, then it might result to damage on their work computers which could easily lead to a massive spread of the worm to other computers in the office through the LAN connection or email. As the effects of the worm were not stated clearly in the article, it is difficult to accurately determine what is at risk. However, assuming the worst, if the incident had taken place at important institutions such as banks or hospitals as an example, valuable information concerning thousands of people be it credit card information or health records could have been compromised. This would not only make the institution a victim but also its customers who had their information stored in the databases of these institutions. In this case, the confidentiality property of the assets would have been reduced. In another situation, the worm could have made changes to the registry of the OS in the victims!| computers leading to permanent damage to the OS which would cause the integrity property of the assets to be reduced. If the worm caused a certain website or service provided by a company to crash then that would be a reduction in data availability. Because the potential effects of this worm are so broad, there is a possibility of reduction in all three CIA properties as a result of this

incident. Threat agents would consist of people who created the worm as well as unsuspecting or trusting users who although do not intentionally cause malice but are still responsible for creating a threat due to their carelessness.

Question 2

1. Scenario 1:
- Assets: Confidential or personal information, i.e. bank account, password, and contact information
- Threats:
Threat Class: Disclosure
Action: Snooping
Users sharing the same WiFi connection might spy on the packets for confidential or personal data that you have sent across the wireless network. Assuming that you are connecting to a wireless connection that does not support any encryption technologies (WEP or WPA), everything sent through or received by your smartphone is in plain text form. The attacker can run some wiretapping tools to collect the data transfer between your smartphone and the recipient. If you are accessing your bank account using this unsecure network, your bank account number and password might leak out.

Threat Class: Deception
Action: Modification
The request you sent across the free WiFi network might be altered. The intruder can read your request to download specialized application from versiontracker.com, and then modify the request packet to certain malicious application instead. The installation of this malicious allows the intruder to gain access of your smartphone without your notice in the future.

- Threats Agents: Any user sharing the same WiFi network that is interested in collecting your personal data, identity theft, hackers or criminal organizations.

2. Scenario 2:
While I am waiting for my friend outside the theater, a person approaches me and demands for my wallet at knife point. At this point, my money, other valuables such as my watch, jewelery, phone and even my life could be at risk. The robber could be satisfied with just my wallet or could even force me to go with him to an ATM machine and withdraw all my money from my account. He might also be dissatisfied with the amount I have and kill me. These can all be considered as threats. Here, the threat agent is the robber because he is intentionally looking to obtain my assets. This threat could be classified as disclosure as I am forced to reveal my bank account's pin number.

3. Scenario 3:
- Assets: Confidential information, such as credit card number and contact information.
- Threats:
Threat Class: Deception

Action: Spoofing or masquerading
In order to shop online, user has to register himself with required information as a member of the site. The user information will be stored in the server!|s database upon registered. However, no one knows how secure the database is. The intruder can spoof himself as the server administrator and gain access to all the private information of the customers of the targeted site. Your information might be one of those being used by the identity theft.

Threat Class: Disclosure
Action: Snooping
Supposed that www.bestbye.com site is using neither SSL nor HTTPS, the credit card information that you have entered are transferred through the network in plain text. The malicious user can easily collect your credit card information while you are sending the information to the recipient

- Threats Agents: Identity theft, www.bestbye.com employees, hackers or criminal organizations

Question 3

1. Scenario 1: The confidentiality property is reduced if my bank account!|s information is retrieved by an unauthorized person. The integrity property is also reduced if my money in the account is illegally transferred to other accounts without me as the owner of the account knowing about it. The availability property could be reduced if the application contained a virus and damaged my phone because I would then have no phone to
use which might cause me severe inconvenience.

2. Scenario 2: In this circumstance, the confidentiality property of the asset is reduced if I am forced to tell the robber my pin number for my bank account. The availability property is reduced because once the robbers takes all my assets then I would no longer have access to them.

Question 4

1. Problem 1:
a. Use firewall software that specializes in DoS attack prevention such as DoSDeflate
b. Install Intrusion Detection System (IDS) to alert that someone tries to access the computer system.
c. Routinely observe system performance
d. Restrict admin / root privilege to prevent website defacement. Instead, only allow specific users such as Web-master to modify website content.

2. Problem 2:
a. Scenario 1:
i. Install firewall on host that is used to access internet
ii. Install anti-virus and anti-spyware on host that is used to do the transaction

iii. Use encryption in sending packets through internet
iv. Try not to access bank account online using public internet connection or in public area
v. Dont use any software from third-party website to access bank account. Instead, go directly to the banks website to do online transaction.
vi. Beware of shoulder surfing when accessing bank information in public area
b. Scenario 3:
i. Install anti-virus and anti-spyware on host that is used to do the transaction
ii. Install firewall on host that is used to access internet
iii. Shop only at reliable and well-known online merchants
iv. Encrypt packets sent through internet