**Assignment 1**

**Written Response Question**

**Q1a)**

Confidentiality is compromised.

A breach of confidentiality happens when information provided by the end user in confidence is supplied to a third party without his/her consent. If Google supplied that information, it would’ve been a breach of the Confidentiality principle.

**Q1b)**

Availability is compromised.

As Google had supplied the information to the FBI, from the bureau’s perspective availability would have been compromised as the flow of data would be disrupted.

**Q1c)**

Privacy is compromised.

Confidentiality is when the user willingly provides data to a third party on the condition that the information isn’t divulged.

Privacy is the right of a person to be left alone and is the more appropriate principle that was compromised. In this scenario, the FBI invaded the privacies of users whose calls were intercepted.

**Q1d)**

Integrity is compromised.

By removing her team’s data from the database of Google’s, she has modified the data in an unauthorized manner which affects the accuracy of the data in the database.

**Q2a)**

Modification. The hacker had hacked Google’s database and removed the data from it.

**Q2b)**

Interception. The hacker’s activity is being monitored by the FBI without their knowledge.

**Q2c)**

Fabrication. The FBI created entries in a database that is virtually indistinguishable from the real thing.

**Q2d)**

Fabrication. Again, the data is being modified and is not distinguishable from the real thing.

**Q3a)**

Deflecting. Plant false information on someone (patsy) to steer the FBI in the wrong direction.

**Q3b)**

Detecting. Monitor the FBI’s communications to prepare for possible raids.

**Q3c)**

Recovering. Become an informant for the FBI in exchange for leniency/immunity from prosecution.

**Q4a)**

Trojan. It spreads when malicious email attachments are opened. Once installed and the user restarts his computer, the program does URL calls to websites owned by the KOVTER developer to generate revenue via click-fraud.

**Q4b)**

Worm. ILOVEYOU is also sent via email attachments as a VBS script file. User who thought that it was a normal txt file would run it which in turn runs the Visual Basic script. This would result in random files on the machine being overwritten. The worm would then spread itself by sending a copy of the script to all email addresses in the Windows Address Book.

**Q4c)**

Worm. Mirai spreads itself by scanning vulnerable IoT devices running Linux and attempting to log into them via factory default usernames and passwords. The infected device then waits on a command and control server which assigns a target for the devices to flood with requests causing a DDoS attack.

**Q4d)**

Worm. NotPetya spreads itself through a variety of methods including a backdoor implemented in an accounting software package (M.E. Doc) which is used by majority in the Ukraine as well as via the EternalBlue and EternalRomance exploits. It masquerades as ransomware with a similar ransom screen as Petya but encrypts files on the computer with no way to revert the encryption.