**3.x Skills building in Cybercrime - International**

**PART 1**

During the course of an investigation related to large scale hacking activities related to banks, the American FBI has been monitoring a hacking forum by using undercover agents and discovers that data from hacked US and European bank accounts is being sold for further exploitation. The FBI conducted an undercover operation and succeeded in buying data (account numbers and PIN and access codes) from a number of different individuals.

As a result of analysing the data the FBI identified two individuals responsible for selling the data; they are Boris Smith, who appears to have been selling such data for a number of years and Teresa Brown who is a more recent member of the forum. Both persons seem to be living in your country (A) but Teresa is a national of your neighbour country (U).

The FBI send information to your 24/7 POC on the bank accounts affected in your country and on Boris and Teresa for further identification. Information was also sent to country U also affected and which has already started an investigation.

**Questions – part 1**

Can you start an investigation in your country based on the information received?

Is the information from the FBI, including information obtained through the undercover operation, admissible as evidence?

If not, what action would you take to secure the information so that it can be used as evidence? Assuming you could start an investigation which potential offences would you be investigating? Explain the roles and decision making responsibilities of your national authorities (24/7 POC, police, prosecutor, judicial authorities at these stages in the process).

**PART 2**

Just as you receive the information from the FBI, one of the biggest banks in your country passes information to your police authorities that several of its customers have been victims of hacking and that money from their accounts has been obtained and transferred to “money mules” in your country and in other countries. This information was gathered by the bank’s IT department in the course of an internal investigation into money transfers and consists of IP addresses, bank account details etc. One of the money mules in your country has been identified as Margaret Jones; she is a national of country U. Some of the bank account numbers provided by the bank match the information sent by the FBI.

**Questions – part 2**

Do you start an investigation against Margaret?

Can you use the information from the bank as evidence? If not what action do you take to secure it? You know that country U has started an investigation, what action do you take with regard to country U?

**PART 3**

You receive information from country U and start an investigation against Boris. During the execution of a search warrant at his home address, Boris is found at his computer but manages to escape. The hacking forum website was displayed on the computer as well as chat sessions with possible hackers offering newly hacked data. Boris also has a gmail account and a yahoo account which was not open on the computer at the time of the search. A paper document next to the computer displays a list of logins and passwords for several gmail accounts, paypal accounts, websites and some bank accounts in your country, and other countries. There are also some documents containing figures and calculations and which implicate Teresa and Margaret. You know that Yahoo has recently opened an office (serving as a regional HQ) in your country.

**Questions – part 3**

What action would you take regarding the hacking forum website and chat sessions – would you view or copy them? (whether you answer yes or no – justify your answer based on your legislative framework).

Are you able to access the gmail accounts using the logins and passwords without obtaining consent from Boris? What action do you take?

What action do you take regarding the yahoo account?

What action do you take regarding the paypal accounts?

What do you do with the bank account information relating to the bank accounts in your country, in other countries?

**PART 4**

Boris is arrested in possession of a false passport at your country’s main airport and Teresa and Margaret are arrested at the border of your country and country G. Country U has issued extradition requests for Teresa and Margaret and the FBI have indicated that the US authorities are interested in having Boris extradited to the US.

**Questions – part 4**

How do you deal with this situation?

**PART 5**

Boris makes some admissions to his involvement with the hacking forum but maintains he was working for Teresa who was in charge of the enterprise. Based on your investigations to data the gmail account is highly significant to proving the full extent of Boris’s involvement.

**Questions – Part 5**

How would you approach google as the service provider?

What sort of information would you need from them? Would your answer be any different if Google had a sales office in your country?

Complete an A 31 template in relation to the request to Google.