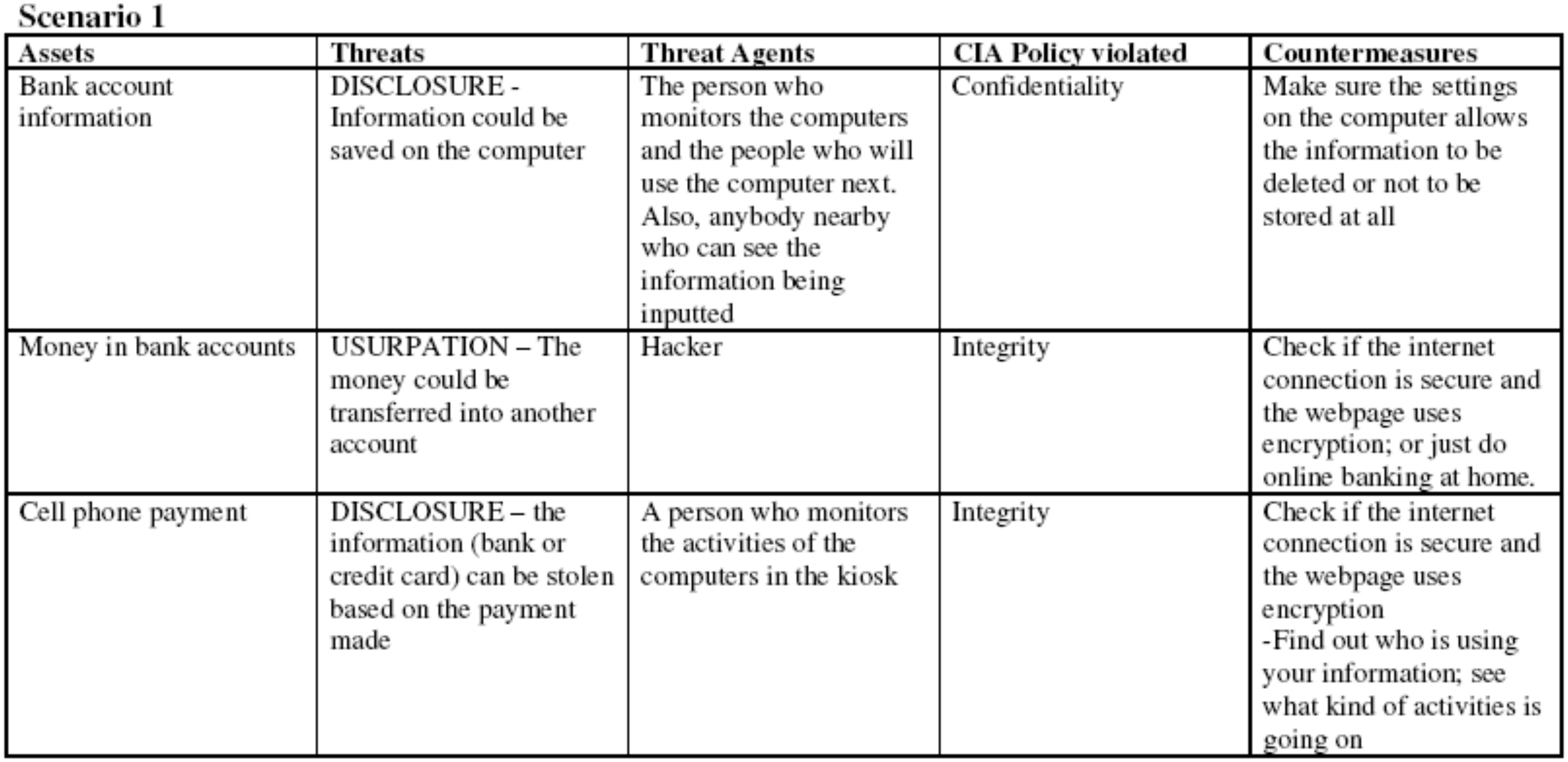
Comments for assignment 1

Sample solution for scenario 1:
You are reviewing your accounts, paying your cell phone bill, and transferring money between your own accounts using online banking system from an Internet kiosk at Vancouver International Airport.

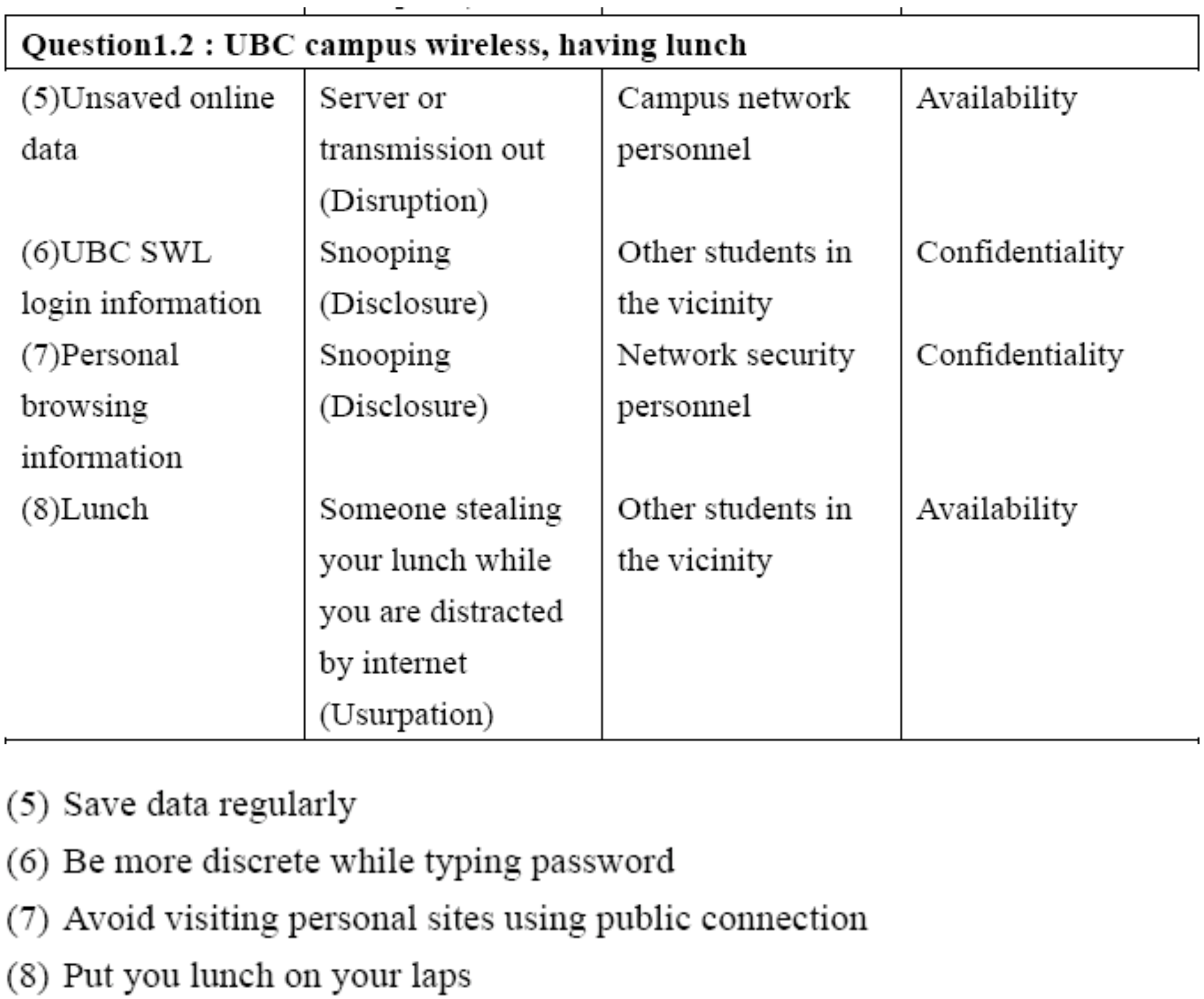


Scenario 1

Assets	Threats	Threat Agents	CIA Policy violated	Countermeasures
Bank account information	DISCLOSURE - Information could be saved on the computer	The person who monitors the computers and the people who will use the computer next. Also, anybody nearby who can see the information being inputted	Confidentiality	Make sure the settings on the computer allows the information to be deleted or not to be stored at all
Money in bank accounts	USURPATION – The money could be transferred into another account	Hacker	Integrity	Check if the internet connection is secure and the webpage uses encryption; or just do online banking at home.
Cell phone payment	DISCLOSURE – the information (bank or credit card) can be stolen based on the payment made	A person who monitors the activities of the computers in the kiosk	Integrity	Check if the internet connection is secure and the webpage uses encryption -Find out who is using your information; see what kind of activities is going on

Contributed by Florence Tabamo.

Sample solution for scenario 2:
You are using UBC campus wireless network at the SUB while having your lunch between classes.



Question1.2 : UBC campus wireless, having lunch			
(5)Unsaved online data	Server or transmission out (Disruption)	Campus network personnel	Availability
(6)UBC SWL login information	Snooping (Disclosure)	Other students in the vicinity	Confidentiality
(7)Personal browsing information	Snooping (Disclosure)	Network security personnel	Confidentiality
(8)Lunch	Someone stealing your lunch while you are distracted by internet (Usurpation)	Other students in the vicinity	Availability

(5) Save data regularly

(6) Be more discrete while typing password

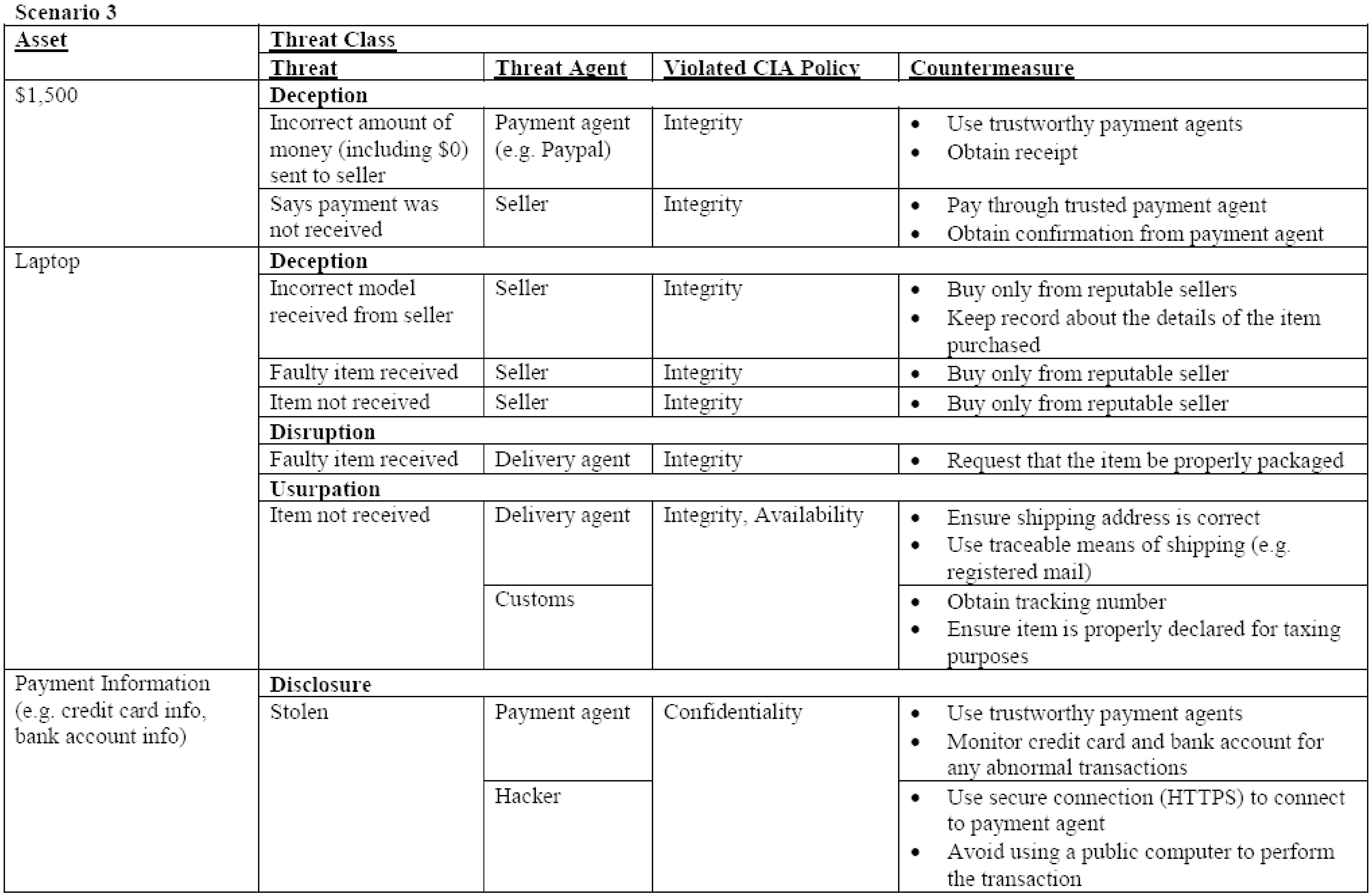
(7) Avoid visiting personal sites using public connection

(8) Put you lunch on your laps

Contributed by Jason Kuo

Sample solution for scenario 3:

You are buying a new Toshiba laptop for $1,500 on an online auction system like eBay.com



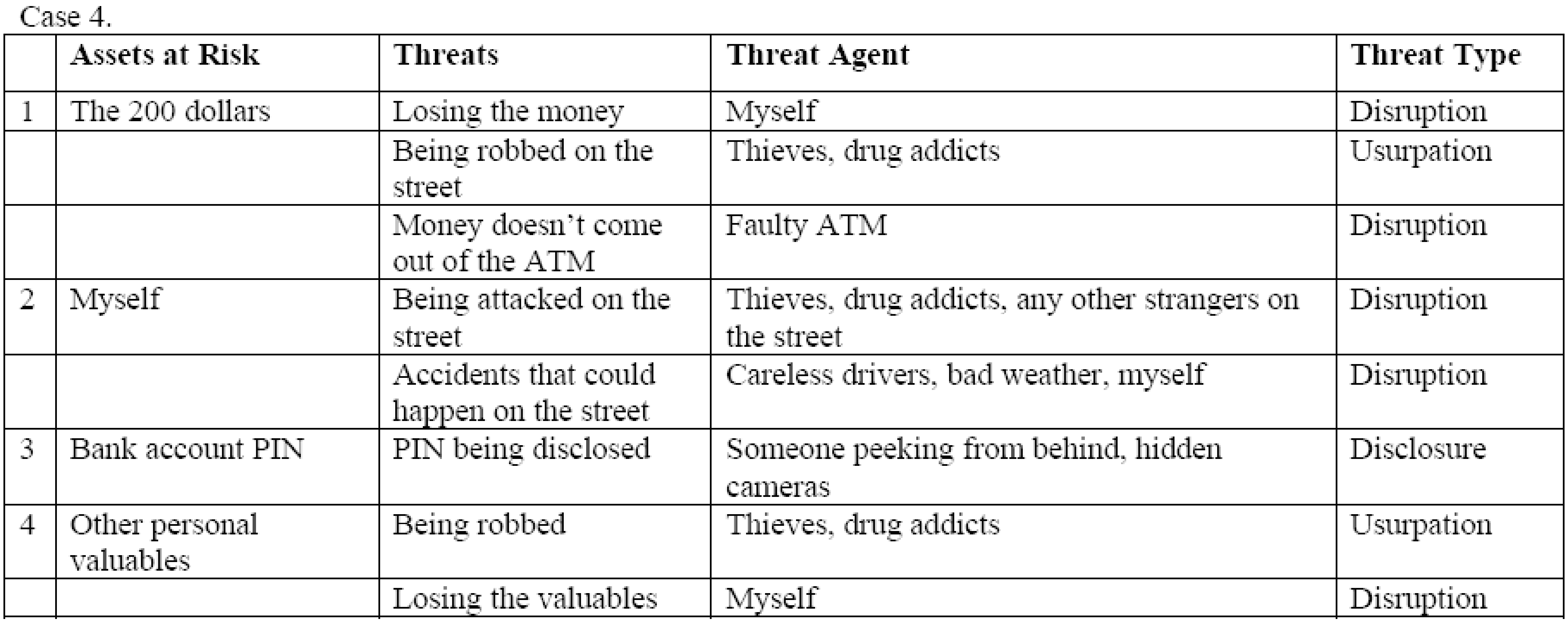
Scenario 3

Asset	Threat Class			
	Threat	Threat Agent	Violated CIA Policy	Countermeasure
$1,500	**Deception**			
	Incorrect amount of money (including $0) sent to seller	Payment agent (e.g. Paypal)	Integrity	• Use trustworthy payment agents • Obtain receipt
	Says payment was not received	Seller	Integrity	• Pay through trusted payment agent • Obtain confirmation from payment agent
Laptop	**Deception**			
	Incorrect model received from seller	Seller	Integrity	• Buy only from reputable sellers • Keep record about the details of the item purchased
	Faulty item received	Seller	Integrity	• Buy only from reputable seller
	Item not received	Seller	Integrity	• Buy only from reputable seller
	Disruption			
	Faulty item received	Delivery agent	Integrity	• Request that the item be properly packaged
	Usurpation			
	Item not received	Delivery agent	Integrity, Availability	• Ensure shipping address is correct • Use traceable means of shipping (e.g. registered mail)
		Customs		• Obtain tracking number • Ensure item is properly declared for taxing purposes
Payment Information (e.g. credit card info, bank account info)	**Disclosure**			
	Stolen	Payment agent	Confidentiality	• Use trustworthy payment agents • Monitor credit card and bank account for any abnormal transactions
		Hacker		• Use secure connection (HTTPS) to connect to payment agent • Avoid using a public computer to perform the transaction

Contributed by Henry Ng

Sample solution for scenario 4:
You are withdrawing $200 from your checking account at an unattended HSBC bank machine at 11:30 PM on East Hastings Street, Vancouver.

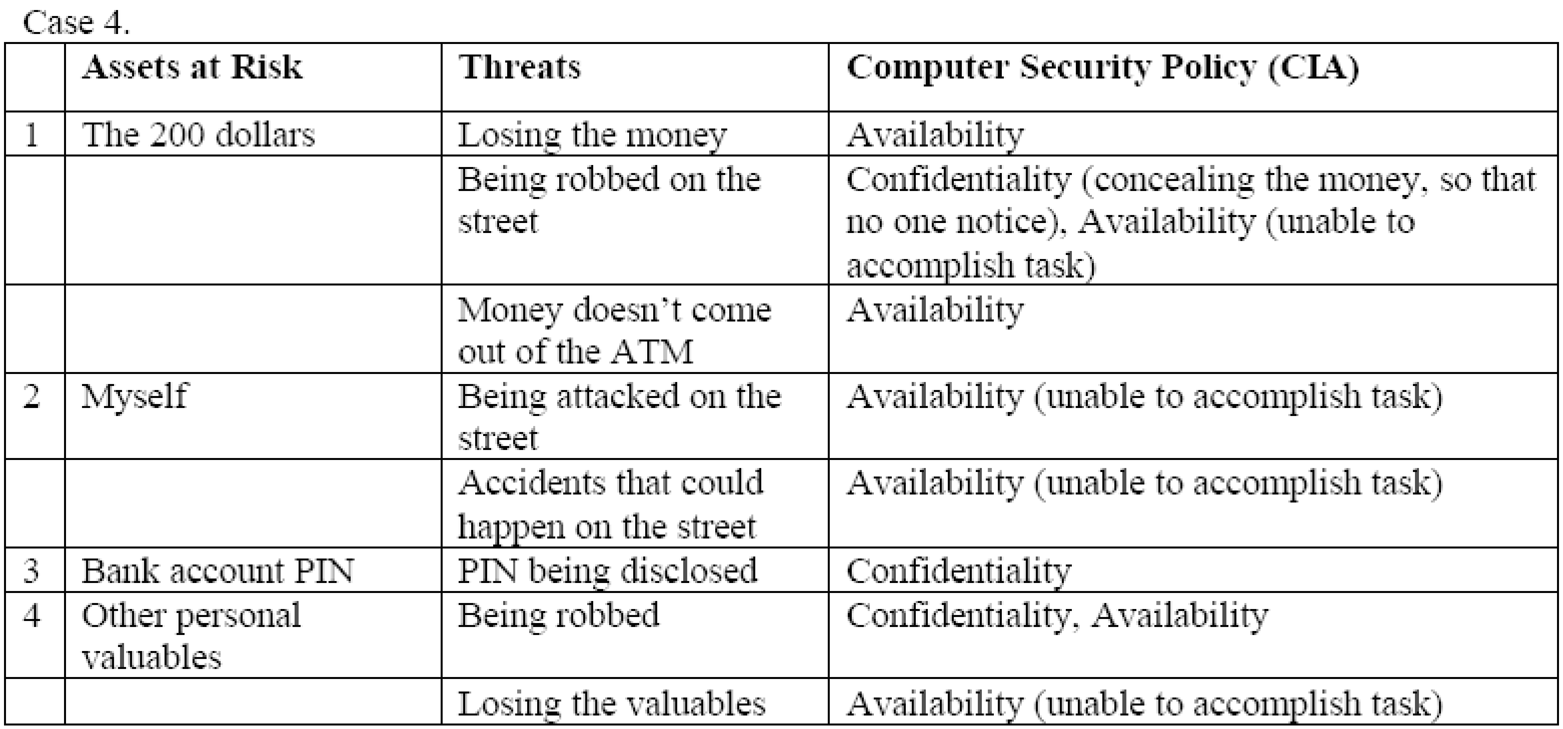
Question 1:



Case 4.

	Assets at Risk	Threats	Threat Agent	Threat Type
1	The 200 dollars	Losing the money	Myself	Disruption
		Being robbed on the street	Thieves, drug addicts	Usurpation
		Money doesn't come out of the ATM	Faulty ATM	Disruption
2	Myself	Being attacked on the street	Thieves, drug addicts, any other strangers on the street	Disruption
		Accidents that could happen on the street	Careless drivers, bad weather, myself	Disruption
3	Bank account PIN	PIN being disclosed	Someone peeking from behind, hidden cameras	Disclosure
4	Other personal valuables	Being robbed	Thieves, drug addicts	Usurpation
		Losing the valuables	Myself	Disruption

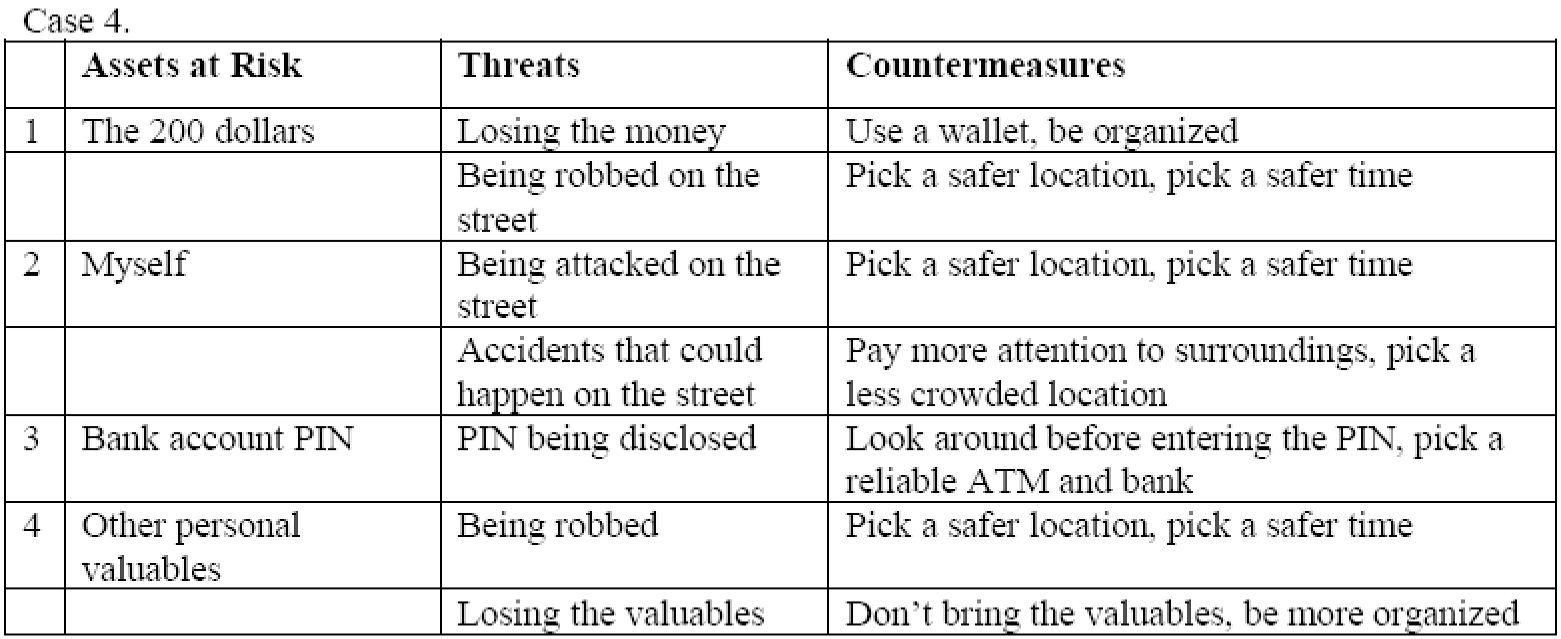
Question 2:



Case 4.

	Assets at Risk	Threats	Computer Security Policy (CIA)
1	The 200 dollars	Losing the money	Availability
		Being robbed on the street	Confidentiality (concealing the money, so that no one notice), Availability (unable to accomplish task)
		Money doesn’t come out of the ATM	Availability
2	Myself	Being attacked on the street	Availability (unable to accomplish task)
		Accidents that could happen on the street	Availability (unable to accomplish task)
3	Bank account PIN	PIN being disclosed	Confidentiality
4	Other personal valuables	Being robbed	Confidentiality, Availability
		Losing the valuables	Availability (unable to accomplish task)

Question 3:



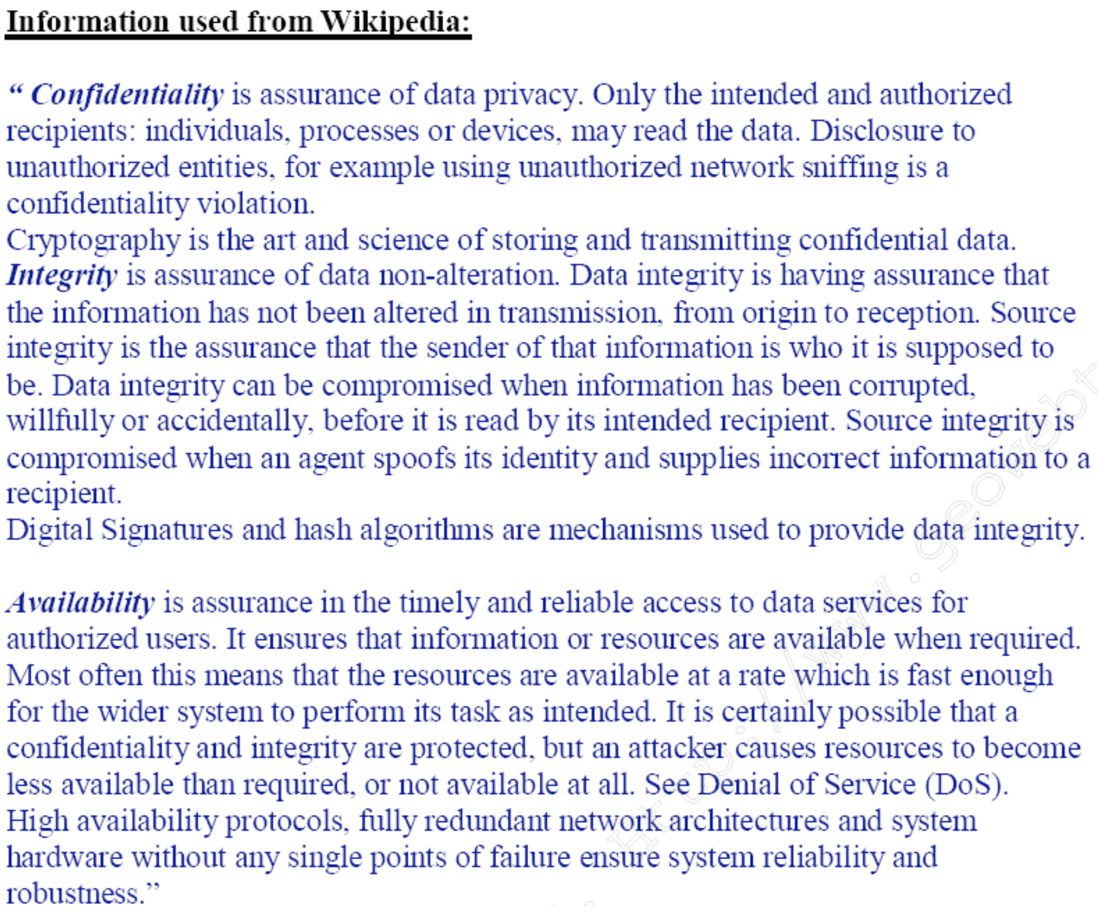
Case 4.

	Assets at Risk	Threats	Countermeasures
1	The 200 dollars	Losing the money	Use a wallet, be organized
		Being robbed on the street	Pick a safer location, pick a safer time
2	Myself	Being attacked on the street	Pick a safer location, pick a safer time
		Accidents that could happen on the street	Pay more attention to surroundings, pick a less crowded location
3	Bank account PIN	PIN being disclosed	Look around before entering the PIN, pick a reliable ATM and bank
4	Other personal valuables	Being robbed	Pick a safer location, pick a safer time
		Losing the valuables	Don’t bring the valuables, be more organized

Contributed by Tik Ning Cheung.

Common problems:

1. The relationship between asset, threat, threat agent, and the corresponding countermeasure is not clear in many submissions.
2. Some people are not clear about the definition of the CIA policy. *Abdel Hamid Ismail Ahmed* found the definition online, which may clarify some of the confusions.



Information used from Wikipedia:

“ ***Confidentiality*** is assurance of data privacy. Only the intended and authorized recipients: individuals, processes or devices, may read the data. Disclosure to unauthorized entities, for example using unauthorized network sniffing is a confidentiality violation.
Cryptography is the art and science of storing and transmitting confidential data.
Integrity is assurance of data non-alteration. Data integrity is having assurance that the information has not been altered in transmission, from origin to reception. Source integrity is the assurance that the sender of that information is who it is supposed to be. Data integrity can be compromised when information has been corrupted, willfully or accidentally, before it is read by its intended recipient. Source integrity is compromised when an agent spoofs its identity and supplies incorrect information to a recipient.
Digital Signatures and hash algorithms are mechanisms used to provide data integrity.

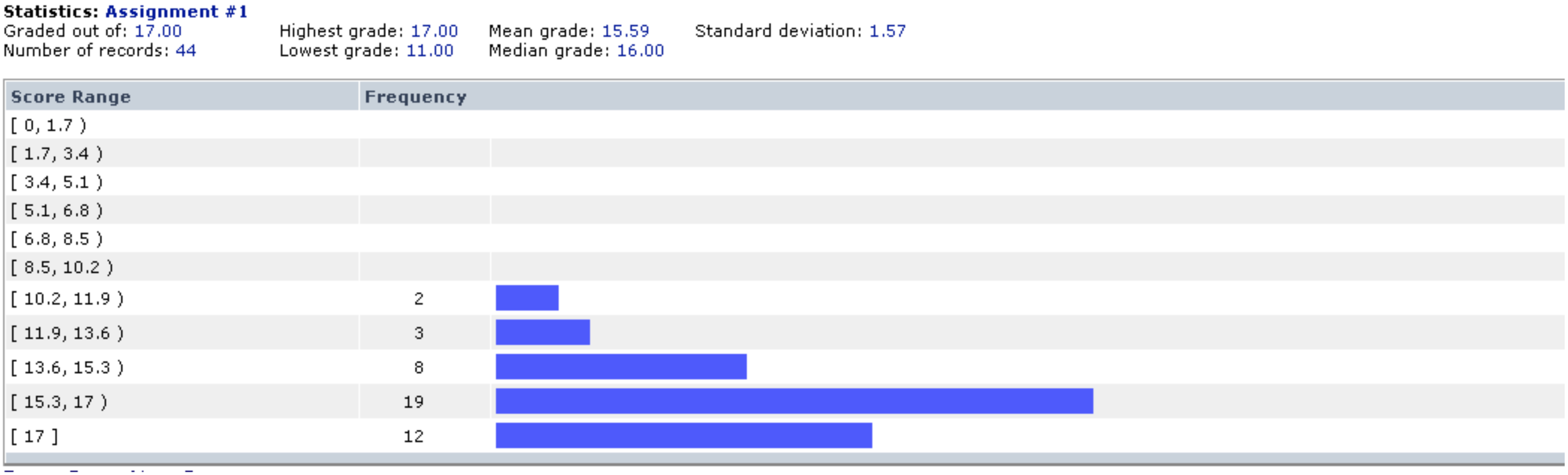
Availability is assurance in the timely and reliable access to data services for authorized users. It ensures that information or resources are available when required. Most often this means that the resources are available at a rate which is fast enough for the wider system to perform its task as intended. It is certainly possible that a confidentiality and integrity are protected, but an attacker causes resources to become less available than required, or not available at all. See Denial of Service (DoS).
High availability protocols, fully redundant network architectures and system hardware without any single points of failure ensure system reliability and robustness.”

3. Some people are not clear about the four types of threats, you can find the definition from the textbook (Bishop), page 4-5. Notice that for physical theft, threat type is usurpation, and the CIA violated is Availability.

4. In scenario 3, one of the threats that missed by many people is swindling, and the threat agent is swindlers.

5. In scenario 4, an important asset is you, because it's almost midnight in a dangerous area (East Hasting).

Grade distribution for assignment 1:



Statistics: Assignment #1

Graded out of: 17.00 Highest grade: 17.00 Mean grade: 15.59 Standard deviation: 1.57
Number of records: 44 Lowest grade: 11.00 Median grade: 16.00

Score Range	Frequency
[0, 1.7)	
[1.7, 3.4)	
[3.4, 5.1)	
[5.1, 6.8)	
[6.8, 8.5)	
[8.5, 10.2)	
[10.2, 11.9)	2
[11.9, 13.6)	3
[13.6, 15.3)	8
[15.3, 17)	19
[17]	12