Question 1

What is the difference between laws and ethics?

* Laws carry the authority of a governing body while ethics do not
* Laws are applicable to everyone while ethics is a personal choice
* Laws are interpreted by court while ethics is interpreted by individuals
* Laws are established by law makers (government) while ethics are presented by religions or group leaders

Question 2

A multi-national software developer with centres in US and Asia is considering developing a policy regarding the ethical use of work resources for personal use. A policy developed for the centres in the US has been very effective and the intent is to use it for all the remaining centres. Explain why the policy developed in the US is unlikely to have the desired outcomes when applied to all centres.

The culture and the definition of ethics are very different in both areas. What might seem ethical to the US might not be seen as ethical in Asia and vice versa.

Unlikely to have desired outcomes due to culture differences.

Read up: ethics and cult behave diff in slides

Question 3

Two of the common claims made by hackers are outlined below:

* A hacker provides a very valuable service to the community because by successfully compromising the security of a system, the hacker is exposing problems with the security setup, problems which need to be addressed.
* There is no actual harm done because everything that a hacker does takes place in a virtual world.

Argue, with the help of examples, against the claims made by the hackers.

\*find weaknesses in the claims and construct counter arguments

1. Breaking into a security system may force changes to the system system but the claim can be easily refuted using 2 basic eg.

Example

* A thief breaks into house bec he could overcome the security system installed, the fact that the house is emptier is not considered as valuable service carried out by the thief.
* It will not be considered a valuable service if someone sets a fire in a cinema full of movie goers because he thought the doors were too narrow for an effective evacuation

1. Although the world may be virtual, the damage is real. The hacker may not have sent a physical letter but the effect will be the same.

Example

* When email information is leaked, but the consequences are very much real and exposed.
* Alth it is a virtual world, if an ID is leaked, it can result to identity theft

Question 4

An employee of a large company is dismissed after his Internet usage showed that he was downloading illegal software, which he was in turn using to do his work. In his defense, the employee claimed that the practice of downloading illegal software was common in his area and could prove that all his colleagues had done the same. Explain whether his defense addressed the ethical component of his behaviour and describe what you feel the company needs to do in terms of the illegal downloads issue, both from the point of view the employee’s termination and the future behaviour of its employees. Justify your reasoning.

The defence does not address the fact that his behaviour was unethical and was sufficient ground for dismissal. Even if everyone was doing something unethical, it does not change the fact that it is unethical. The employee should have reported unethical behaviour of the colleagues instead. The fact that the other employees could still do so, did not mean that it was accepted by the organisation. It was only because the organisation had not done enough to prevent that from happening.

Example

It is not ok to share passwords in an organisation, no matter the number of employees who share the same password. If it is known that a group of employees are sharing the same password and it violates the company policy, one should report it to management instead of allowing the practice to continue.

The company needs to address what is fundamentally a lack of care in terms of what is ethical when it comes to internet and software usage.

* The employee’s termination stands and all the other remaining employees need to be trained in what is ethical behaviour and regards to internet as well as software usage.
* The company’s policy and its dissemination needs to be reviewed and the penalties need to be strictly enforced

Question 5

A programmer, who was assigned as a sole person to work on an existing banking system, discovered a loophole that the system did not properly record small withdrawals from automatic teller machines (ATMs) around mid-night. This allowed a customer to withdraw small amount of money at a time without affecting the account balance. The programmer did not inform the bank, but instead inserted his own scripts into the banking system to suppress the generated alerts. He then took a large sum of money by performing thousands of withdrawals over several years without being detected, until later when his code was identified and removed in a security audit

* Identify and discuss three (3) ethical and/or legal issues in this example.
* Suggest three (3) actions that could have been done by the bank to prevent such an incident from happening.

This is a slicing attack - method where programmer inserts a code and are able to withdraw small amt of money fr bank wo being detected

Issues

1. Criminal issue - insert malicious code in system
2. Criminal issue - Exploit vulnerability to his own benefits
3. Ethical issue - Programmer did not notify the bank of the loophole

Suggestion

1. Freq audits to det mal activity
2. Banks assign more than 1 person to do a job

Rotation of duties ensures integrity.

Employees will not be able to get the job done without each other

1. Education and training, create severe penalty to avoid that from happening

Deterrent control, eg. penalty