COM6655 Professional Issues Exam 2020/21

SOLUTIONS

You should regard these as "solution sketches" – the main points are covered, indicating where marks are allocated. It should go without saying that when answering the exam you should write answers that are in coherent sentences (not in the note form used below).

Question 1

(a) (i) Utilitarianism – the action is right that promotes the greatest good [5%]. You could argue utilitarianism in various ways, e.g. that the hackers are likely to keep/use the data anyway therefore the interests (happiness) of customers outweighs their own [5%]. You could also potentially argue that if the hackers could be trusted, it was right not to inform customers since to do so would cause them anxiety. Having a logical argument here is more important than the particular stance taken.
(ii) Kantian ethics – the categorical imperative, treating people as ends (respecting their rights) and not merely as means [5%]. JohnnyCab have used customers merely as means (not respected their rights/desires) – it was not the right action [5%].

(b) The answer requires a focused explanation of the principles that apply in the scenario, not a simple listing of all data protection principles. A good answer will note the following:

The relevant legislation is the GDPR as implemented by the Data Protection Act 2018 [5%]
JohnnyCab is the data controller – brief explanation [5%]
MegaCloud is the data processor – brief explanation [5%]
You should argue that the data concerned meets the requirement of being personal data (name, location etc) [5%]
JohnnyCab is keeping data for a long time – this may break principles 5 (storage limitation) of the GDPR; you might otherwise argue that customers must have given permission for storage over the long term [5%]
Customers need to have given permission for their data to be used for analysis [5%]
Principle 6 (integrity and confidentiality) has been breached –MegaCloud do not appear to have had adequate security measures (well-known weakness had not been patched) [5%]
By not recording and reporting a data breach of which they are aware, JohnnyCab are in breach of principle 7 (accountability) [5%]

(c) In 1985 there was no legislation specific to hacking. Relevant legislation is the fraud offences in the Theft Act 1968 and 1978 [5%].
Some discussion needed about the applicability of these to the scenario, e.g. JohnnyCab are not permanently deprived of the data (they still have it), and deception of a human mind is required [5%].
By 2005 we have the Computer Misuse Act (1990) [5%].
Relevant offence is section two, Unauthorised Access with intent to commit or facilitate a further office – and you should identify that the further offence is blackmail [5%]

(d) You should briefly explain what the law of confidence is [5%].

You need to reason whether the data concerned has the necessary quality of confidence about it – yes, because it is personal data and on a (supposedly secure) server [5%].
They could seek an injunction to prevent distribution of the data [5%].
In practice the legal protection is weak – some discussion of this (e.g., they can't identify the hackers; if data is placed on the internet they have no means of action against people who distribute it further and were not aware that an obligation of confidence was imposed) [5%]

Question 2

(a) Advantage is that, at least in principle, they can increase quality or reduce costs [5%] therefore gaining an edge in a competitive market [5%].
Deskilling will be an issue [5%] which could lead to reduced productivity and demotivation [5%].
Advice would likely be to match the ongoing organisation to the new technology, e.g. with a reference to sociotechnical design [5%].
Involve employees in decisions about how to use the new technology [5%].
Consider teams that work on sub-units of production and rotate around jobs [5%], which is more resilient to failure (since employees have an oversight of the whole manufacturing process) [5%].
Credit will be given for raising other relevant issues, e.g whether it is possible to retrain current employees.

(b) (i) Contracts exist between the injured employee and DWC (contract of employment) and between DWC and BigBot [5%].
You should identify that the latter is a contract for a service and is subject to the Sale of Goods and Services Act 1982 [5%].
This implies terms into the lease agreement requiring that it be carried out with a reasonable degree of care and skill [5%].
You should discuss what is "reasonable" in this scenario (e.g., is it "reasonable" to expect that software should be completely free of errors?) [5%].
Exclusions under this contract are limited by the Unfair Contract Terms Act 1977 [5%]. The claim by BigBot that they can exclude liability for injury does not hold up if it can be shown that they were negligent [5%].
A good answer will refer to the concept of vicarious liability (is the robot like an "employee", and therefore is DWC liable for its actions?)

(ii) You should reason about whether DWC and BigBot owe a duty of care to the injured employee – this will depend on whether the injury was reasonably foreseeable [5%].
Were DWC negligent in allow the robot and human operator to work in close proximity, despite the manufacturer's caution? – some discussion on this point [5%].
Would need show that the error in the control software was negligence, ie that it would not have been made by a competent professional. [5%]
A good answer will refer to the concept of contributory negligence (e.g. liability of BigBot could be reduced because of DWC's actions in ignoring the safety warning) [5%]

(iii) Relevant legislation is the Consumer Protection Act 1987 [5%].
Some discussion of whether this applies (since the injured employee is not a "consumer"), and the relevance of the "state of the art" defence [5%].

Question 3

(a) (i) Relevant legislation is the Copyright, Designs and Patents Act (1988) [5%].
Decompilation is provided for by the Copyright (Computer Programs) Regulations (1992) [5%] but in this case the decompilation right does not apply because its purpose was to make a competing product [5%].
It is irrelevant that they rewrote the program in a different language; merely the act of decompiling the program was an infringement of copyright [5%].
A good answer will point out that decompilation and manual rewriting are both effectively translation, which is a restricted right [5%].

(ii) Probably infringement, since copyright extends beyond literal similarity to the structure of the program [5%]
A good answer will mention relevant case law, e.g. IBCOS vs Barclays Mercantile (1994) [5%] The test suggested in Computer Associates vs Altai should be mentioned [5%] – this would indicate whether copying took place in this case, a brief discussion of this.
Although the Z-buffer algorithm is very similar this is probably "code dictated by function" – since it is a standard algorithm [5%], hence there is no expression to be copied [5%].

(iii) The idea is not protected by copyright, which only protects expression [5%].
Screen designs and icons can be protected by copyright [5%]
Some discussion needed here on "look and feel" as a criterion for infringement [5%] with reference to relevant case law such as Whelan vs Jaslow and Apple vs Microsoft [5%].
Possible infringement – although contentious given different case law, e.g. Flanders vs Richardson [5%]

(b) (i) You should refer to Beta vs Adobe (1996) as relevant case law [5%]
Case law indicates that the contract for supply of the software (licence) is not separate from the contract for supply of the physical media (contract of sale) [5%]
The actions of Rainforest are not justified – the licence is part of the contract of sale, it is a single contractual arrangement [5%]

(ii) Yes. Relevant legislation is the Copyright (Computer Programs) Regulations (1992) [5%]. This gives a right to make a backup copy if it is necessary for lawful use – the term in the licence is irrelevant [5%]. A good answer will refer to the specific section of the Act (296A).