**Answers**

1. Ben works for a large insurance company. He commutes daily from Norwich to London and works on his laptop during the train journey. He has access to customer data stored in the “cloud”.

(a) Describe **two** methods by which a virus may be introduced into the company’s network via Ben’s computer. [4]

Ben can open an email with an infected attachment. (1) When the attachment is opened the virus is run. (1)

A phishing email can encourage Ben to go to a website (1) where the virus is downloaded to his computer (1)

A virus on Ben’s laptop can be transferred to the company systems / server (1) when he connects to it (via VPN / Wi-Fi / network cable) (1)

(b) Describe **two** methods by which the personal data of individual customers could be stolen by criminals. [4]

Up to **two** marks for each of the following techniques:

The laptop could be stolen (1) whilst on the train / walking to the office or home (1) the hard drive can be removed / the password can be cracked (1) so that the customer data can be accessed. (1)

A backdoor / spyware can be installed (1) which allows a hacker to access the computer remotely (1) and upload the personal data to their computer. (1)

A phishing email / social engineering could obtain his username and password (1) this would allow the hacker to log in to his computer remotely (1) and obtain files with the customer data. (1)

(c) Discuss how the theft of personal data may affect the customers and the company. [8]

Effect on the customers

* Customers may have their identities stolen.
* Personal details such as name, address, birthdate can be used to produce fake ID / open bank accounts / apply for credit cards.
* It will be possible to use bank account details / credit card details to spend money or get into debt.
* Bad debt could lead to a bad credit rating.
* This will make it hard to get a mortgage or loan.
* It will take time for the customer to solve the effects of any identity theft.
* They may receive infected emails from the criminals.
* Or their details may be sold and they then become the target for spam, advertising or phishing attacks.
* They may suffer stress and have to spend large amounts of time solving the problems.

Effect on the company

* The company will suffer a loss of reputation.
* Customers may move to a competitor.
* The company may have to pay compensation.
* The company would have breached the Data Protection Act which could result in penalties.
* The company may be fined by the Information Commissioner’s Office.

|  |  |  |
| --- | --- | --- |
| * L
 | Mark | Descriptor (award up to 6 marks) |
|  | 0 | No rewardable material |
| Level 1  | 1–2 | Demonstrates isolated elements of knowledge and understanding, with major gaps or omissionsFew of the points made will be relevant to the context in the questionLimited discussion which contains generic assertions rather than considering how the theft of personal data could affect the customers and company. |
| Level 2 | 3–5 | Demonstrates some accurate knowledge and understanding, with only minor gaps or omissionsSome of the points made will be relevant to the context in the question, but the link will not always be clearDisplays a partially developed discussion which considers some of the techniques and some consideration of how the theft of personal data could affect the customers and company. |
| Level 3 | 6–8 | Demonstrates mostly accurate and detailed knowledge and understandingMost of the points made will be relevant to the context in the question, and there will be clear linksDisplays a well-developed and logical discussion which clearly considers how the theft of personal data could affect the customers and company. |

2. Jonas is trying to visit a website which is working very slowly. Sometimes the pages are not being served to him at all. A news site says that the website is currently undergoing a Denial of Service attack.

Describe how a Denial of Service attack occurs. [4]

Many computers send unnecessary packets / requests to a server. (1) This is known as a flood. (1) These computers will usually have been taken control by a hacker (1) creating what is known as a botnet (1). The server cannot process requests fast enough (1) so legitimate requests are not served / the website operates slowly or not at all (1)

[Total 20 marks]