- No calculator permitted in this examination

THE UNIVERSITY OF BIRMINGHAM

THIS PAGE TO BE REPLACED BY OFFICE

06 28213

Secure System Management

RESIT

September 2016 1 hour 30 minutes

[Answer ALL questions]

1. An enterprise responds to risks to its security with a *risk treatment plan*. As part of this, it might decide to *transfer* or *accept* some risks.

   (a) Describe two ways in which risks associated with credit-card processing might be transferred to another party. **[8%]**

   (b) Describe one way that risks associated with equipment failure sufficient to bring the enterprise to a halt might be transferred. **[4%]**

   (c) Accepting risks involves analysing the cost of reducing or mitigating a risk, and comparing it with the likelihood and impact of the risks occurring. How should a business record its acceptance of a risk? Who should be involved in recording and accepting the risk? What is the name of the document which records the risks the business is accepting? **[6%]**

   (d) A business is concerned that data stored on mobile devices may be revealed to competitors. You are asked by the security officer to evaluate the benefits of *encrypting* these devices, such that all data stored on them requires knowledge of a passphrase to decrypt. Write a short report which:

   - Outlines two risks that encryption treats; **[4%]**
   - Outlines two risks that encryption does not treat; **[4%]**
   - Summarises your advice to the security officer on the benefits of device encryption. **[6%]**

2. Risk assessments sometimes distinguish between the *motivation* and the *capability* of attackers.

   A company which manufactures chocolate is performing a risk assessment:

   (a) Describe two types of attacker who would have capability at the upper end of the scale, but would be assumed to have low motivation. **[6%]**

   (b) Describe two types of attacker who might have a very high motivation, but whose low capability would make them a small risk to an enterprise. **[6%]**

   (c) If a risk assessment does not consider motivation, what will be the effect on the overall conclusions of the risk assessment? **[6%]**

3. A company which holds an ISO 27001 certificate finds that its network has been compromised. A routine check in the CEO's office suite finds that his personal assistant's machine has been infected with a keylogger.

   (a) As part of the ISO 27001 certification there will be a procedure to be followed in the event of an IT compromise. Give four items that such a procedure should contain. **[8%]**

   (b) What actions should the business take after the immediate problem — the keylogging software — has been resolved? **[8%]**

(c) What is meant by a *root cause analysis*, and why is it important that one be performed in this case? **[8%]**

4. A common technique for controlling financial risk is *segregation of duties*, which prevents (for example) the same person from adding a new supplier to the system and then approving payments to that supplier.

   In the context of a company which uses segregation of duties to control financial risk:

   (a) Why is it important that users do not share usernames and passwords? What measures could be taken to make it harder for such sharing to happen? **[10%]**

   (b) What operational problems may be caused by users (correctly) refusing to share credentials? What changes might be required to a system of IT controls so that users do not feel the need to share credentials? **[10%]**

   (c) How effective do you think segregation of duties is as a control in small companies whose staff are all in one office? Explain your answer. **[6%]**