

COMPUTER SCIENCE TRIPOS Part IA – 2021 – Paper 2

5 Software and Security Engineering (rja14)

A company has fired one of its senior staff after an incident that they claimed was an accident, but where the directors suspected malice. The company's auditors have suggested a review of the company's systems to mitigate 'the insider threat', and your advice has been sought. The directors want to be able to assure the shareholders that they are taking all reasonable steps to limit the damage that staff could do to affect the company's share price, whether accidentally or otherwise.

- (a) Describe a multilevel security policy briefly, explaining what sort of harms it seeks to prevent, and how. [5 marks]
- (b) Describe a separation-of-duty security policy briefly, explaining what sort of harms it seeks to prevent, and how. [5 marks]
- (c) Describe one approach to minimising the risk of user error that is based primarily on psychology. [5 marks]
- (d) Introducing architectural changes to the company's information systems will take time, while changes to user interfaces and workflows are often simple to implement. Which psychological approaches might be adopted more quickly, and what might you expect to go wrong? [5 marks]