The follow questions are a random assortment of questions which may or may not be in the exam. The questions are provided purely for you to evaluate your knowledge and understanding of the subject matter. Furthermore, the questions do not represent the structure of the exam, nor should you rely on the sample questions as your only focus of study. Answers to the following questions will not be provided.

1. Discuss the advantage(s) and disadvantage(s) of security vulnerabilities being made public as soon as they are discovered.

2. Describe the security advantages of the NTFS file system.

3. Biometric technology has been available for a number of years; however its adoption has been slow. Discuss the factor(s) that you see as inhibiting or delaying the adoption of biometric technologies. Also include in your answer any factor(s) that might increase the adoption of biometrics.

4. Discuss the similarities and differences between symmetric and asymmetric encryption. Include in your answer a discussion of the strengths and weaknesses of both.

5. Describe the privacy issues surrounding the use of RFID tags.

6. Discuss the role(s) played by certificates and Certifying Authorities (CAs) in the process creating and verifying digital signatures.

7. Discuss in depth the difficulty involved with the creation of consistent, industry wide naming conventions for new malware.

8. Discuss the range of security measures that you would recommend to improve the security of a home PC connected to the internet using a broadband connection.

9. Using the goal of "Access Confidential Information" draw an attack tree depicting the different ways by which an attacker could access confidential information from a home user's Windows computer. Assume no computer or network security has been implemented.

10. Describe how you could use Google for reconnaissance.

11. Explain how you could reduce the amount of time require to perform a brute force attack?

12. Describe the purpose and limitations of the program Steghide.

13. Discuss the advantages of Governments being able to restrict end-users from using cryptography.

14. From a security perspective, discuss the disadvantages of open source operating systems.

15. Describe the security issues when using the program KeePass?

16. Describe the security advantages of the NTFS files system.

17. Describe measures that can be taken to dispose of magnetic media appropriately.

18. Describe the characteristics and functionality of digital signatures.

19. Describe the issues and trends associated with the deployments of botnets.

20. Assuming that an attacker can capture a hashed password, discuss in depth the ways in which he/she could minimise the time necessary to crack the password through technical means.

21. Identify and discuss the issues that would need to be considered when determining a suitable backup strategy for a medium to large organisation. Do not provide an actual backup strategy; discuss the issues that would need to be taken into consideration.

22. Briefly describe the difference between a rootkit and ransomware?

23. What are the potential benefits of the program PC-Time?

24. Briefly describe what would happen if you copy two 60MB files one after another into a 100MB Truecrypt file container.

25. Governments should be able to restrict end-users and large corporations from using cryptography. Discuss the advantages and disadvantages of such a proposition.

26. Biometric technology has been available for a number of years; however its adoption has been slow. Discuss the factor(s) that you see as inhibiting or delaying the adoption of biometric technologies. Also include in your answer any factor(s) that might increase the adoption of biometrics.

27. From a security perspective, discuss in depth the advantages and disadvantages of open source versus closed source (commercial) operating systems.

28. Discuss in depth the issues surrounding the disposal of magnetic media such as hard drives by a large organisation. Include in your answer a discussion of the risks involved and the measures that can be employed to reduce these risks. Also include in your answer a discussion of the problems with implementing these measures.

29. Discuss in depth the similarities and differences between symmetric and asymmetric encryption. Include in your answer a discussion of the strengths and weaknesses of both.

30. Discuss in depth the issues and trends associated with the deployments of botnets. In your discussion, briefly show what a botnet is and how it works. Present examples of its use and the dilemmas that home users and businesses face as a result of the growing number of botnets on the Internet. You may use diagrams or tables to further portray your answers.