Making IT good for society

BCS Level 4 Certificate in Cyber Security Introduction QAN 603/0830/8

Specimen Paper A

Record your surname / last / family name and initials on the answer sheet.

Specimen paper only 20 multiple-choice questions – 1 mark awarded to each question. Mark only one answer to each question. There are no trick questions.

A number of possible answers are given for each question, indicated by either **A. B. C. or D**. Your answers should be clearly indicated on the answer sheet.

This qualification is regulated by Ofqual (in England).

1. Which of the following are required for a ransomware attack to be successful?

a) Sending an e-mail that looks genuine with an attachment to a user.
b) Luring a user to click a link and download a file.
c) Exploiting a poorly configured firewall.
d) Disrupting power supply of the server backups.

A a and b only.
B c and d only.
C a, b, c and d.
D b, c and d only.

2. What does CIA represent in relation to cyber security?

A Confidentiality, identity, availability.
B Confidentiality, integrity, availability.
C Confidentiality, integrity, accessibility.
D Criminality, integrity, availability.

3. What sort of control is anti-virus software?

A Procedural.
B Perceptive.
C Protective.
D Primitive.

4. Which device is designed **PRIMARILY** to direct traffic on a network to a designated IP address?

A Hub.
B Firewall.
C Router.
D DMZ.

5. Which of the following is **TYPICALLY** a feature of a thick client?

A Uses a server for the main processing activity.
B Does the bulk of the processing activity rather than the server.
C Its designed for use by very inexperienced people.
D Uses web-based software through the terminals.

6. Which of the following may need to be reviewed when the threats landscape changes?

a) Security objectives.
b) Security requirements.
c) Security budget.
d) Security policy.

A b, c and d only.
B a, b and c only.
C a, c and d only.
D a, b and d only.

7. Which of the following are impacts of a cyber attack on a business?

a) Financial losses.
b) Reputational damages.
c) Use of office supplies.
d) Legal consequences.

A a and d only
B a, b and c only.
C a, b and d only.
D b and d only.

8. Fill in the blank:

A technique used by risk managers for forecasting future events, such as accidental and business losses, is called _____.

A Competitor analysis.
B Risk analysis.
C Trend analysis.
D Cost benefit analysis.

9. What do we call those parts of the World Wide Web whose contents are **NOT** indexed by standard search engines for any reason?

A Surface web.
B Darknets.
C Tor network.
D Unallocated spaces / clusters.

10. Which of the following security assurance models could **NOT** be evaluated by existing security evaluation criteria?

A Intrinsic assurance.
B Extrinsic assurance.
C Implementation assurance.
D Operational assurance.

11. What is the Common Criteria?

A An international standard for ICT product security certification.
B A way of checking if the most important security controls are in place.
C The easiest security controls to implement in an ICT system.
D Standard clauses expected to be seen in an outsourcing contract.

12. Which of the following is a DNS technique used by botnets to hide phishing and malware delivery sites behind proxies?

A Fast flux.
B IP spoofing.
C Distributed denial of service.
D Logic time bomb.

13. Fill in the blank with the **MOST LIKEY** answer.

If a company fails to deliver an agreed service to its customers, then it may be a breach of _____.

A Cyber law.
B Criminal law.
C Civil law.
D Contract law.

14. The following activities are parts of the attack chain principle. In which order do they **NORMALLY** happen?

a) Weaponsiation.
b) Actions on objective.
c) Delivery.
d) Reconnaissance.

A c, d, b, a.
B d, a, c, b.
C d, b, a, c.
D c, d, a, b.

15. What **SHOULD** be the **MAIN** focus of information security practices in any organisation?

A Implementing security controls.
B Aligning with the business objectives.
C Remaining cost effective.
D Deploying long term solutions.

16. Which of the following are **GENERALLY** considered to be reliable source of research outcomes and industry practice?

a) Peer reviewed journals.
b) Conference proceedings.
c) Professional body whitepapers.
d) Online chatting forums.

A a, b and c only.
B a, b, c and d.
C b, c and d only.
D a and d only.

17. Which of the following is **LEAST LIKELY** to be an information security risk introduced by a Bring Your Own Device (BYOD) programme?

A BYOD devices could provide unauthorised access to office systems through their inter-connectivity.
B BYOD devices could be used to spread malware to office systems by transferring viruses through their connections to office networks.
C BYOD devices could provide accurate details of the user's location, thereby facilitating directed attacks on staff members.
D BYOD devices could have a serious effect on the volume of network traffic on an office system to which they are connected.

18. When are service providers required by UK law to notify the Information Commissioner's Office (ICO)?

A If a company's chief information officer is replaced.
B If a breach of personal data occurs.
C If a customer's information is kept for more than 90 calendar days.
D If a customer's bank details are not received within 24 hours of a sale.

19. Poor system configuration issues can be identified by evaluating the system, using which of the following?

A Privacy enhancing techniques.
B Horizon scanning.
C Business impact analysis.
D Penetration testing.

20. What is horizon scanning?

A Looking at developments in technology to try and identify future trends or issues.
B Identifying known threats appearing on the boundaries of a company's network.
C Determining what new inventions in technology your competitors are bringing to market.
D Scanning for vulnerabilities in the software that has been installed on the company's networks.

-End of Paper-